www.elettronica-plus.it

EMBEDDED

MAGGIO 2018 **68**

LA COPERTINA di EMBEDDED

I sistemi di visione embedded, dalla complessità alla semplicità

SPECIALE

Starter kit per progetti IoT
Sensori sempre più intelligenti

FIERA MILANO MEDIA

Supplemento a Elettronica oggi n° 470 - Novembre-Dicembre - In caso di mancato recapito inviare al CMP/CPO di Roserio-Milano per la restituzione al mittente previo pagamento resi

ecia
MEMBER
ecsn
member
CEDA

SOMMARIO

Per superare le sfide legate alla visione integrata, Avnet Silica e Xilinx sono congiuntamente impegnate a offrire kit di progettazione e progetti di riferimento che hanno l'obiettivo di ridurre la complessità software e hardware. La natura programmabile degli strumenti proposti riduce la complessità dello sviluppo portandola al livello dei progetti basati su processore. Con un ambiente di programmazione più semplice, è possibile lavorare sul software e quindi ottimizzare l'hardware attorno a una soluzione.

Avnet EMG Italy S.r.l.
Via Manzoni, 44
20095 Cusano Milanino (MI)
Tel. 02660921
www.avnet.com
milano@avnet.eu

Redazione **Carlo Antonelli** Direttore Responsabile
Filippo Fossati Coordinamento Editoriale
filippo.fossati@fieramilanomedia.it - tel: 02 49976506
Segreteria di Redazione - eo@fieramilanomedia.it

Collaboratori: Antonella Pellegrini, Richard Bellairs, Lee Cresswell, Emanuele Dal Lago, Martin Danzer, Alberto Di Paolo, Rudolf Dienstback, Peter Fairhurst, Francesco Ferrari, Giorgio Fusari, Aldo Garosi (disegni), Silvano Iacobucci, Sergio Insalaco, Lucio Pellizzari, Arno Stock, Michael Uyttersprot

Pubblicità **Giuseppe De Gasperis** Sales Manager
giuseppe.degasperis@fieramilanomedia.it
tel: 02 49976527 - fax: 02 49976570-1
Nadia Zappa Ufficio Traffico
nadia.zappa@fieramilanomedia.it - tel: 02 49976534

International Sales
U.K. – SCANDINAVIA – NETHERLAND – BELGIUM
Huson European Media
Tel +44 1932 564999 - Fax +44 1932 564998
Website: www.husonmedia.com
SWITZERLAND - IFF Media
Tel +41 52 6330884 - Fax +41 52 6330899
Website: www.iff-media.com
USA - Huson International Media
Tel +1 408 8796666 - Fax +1 408 8796669
Website: www.husonmedia.com
GERMANY – AUSTRIA - MAP Mediaagentur Adela Ploner
Tel +49 8192 9337822 - Fax +49 8192 9337829
Website: www.ploner.de
TAIWAN - Worldwide Service co. Ltd
Tel +886 4 23251784 - Fax +886 4 23252967
Website: www.acw.com.tw

Grafica e fotolito **Emmegi Group** – Milano
Stampa **FAENZA GROUP** – Faenza (Ra) • Stampa

Aderente a: ANES ASSOCIAZIONE NAZIONALE EDITORIA DI SETTORE

Proprietario ed Editore

FIERA MILANO MEDIA

Fiera Milano Media
Enio Gualandris • Presidente
Carlo Antonelli • Amministratore Delegato
Sede legale • Piazzale Carlo Magno, 1 - 20149 - Milano
Sede operativa ed amministrativa
SS. del Sempione, 28 - 20017 Rho (MI)
tel. +39 02 4997.1 fax +39 02 49976573 - www.tech-plus.it

Fiera Milano Media è iscritta al Registro Operatori della Comunicazione n° 11125 del 25/07/2003.
Autorizzazione alla pubblicazione del tribunale di Milano n° 129 del 7/03/1978.

EMBEDEDD **68**

INSERZIONISTI

SOCIETÀ PAG.

SI PARLA DI...

Embedded computing sempre più pervasivo

Nel corso di quest'anno si assisterà presumibilmente a un'interessante evoluzione nel campo dell'elaborazione embedded che troverà sempre più spazio in applicazioni quali networking, sicurezza informatica e Industrial Internet of Things. Per tutti coloro che operano nei settori industriale e commerciale la protezione delle reti e del loro "patrimonio" di dati è divenuto un aspetto sempre più rilevante. Complice la costante minaccia di potenziali attacchi informatici, il focus sarà la protezione dei sistemi di controllo industriale (ICS - Industrial Control System), soprattutto quelli che gestiscono asset strategici: erogazione di servizi di primaria utilità, sottostazioni di distribuzione dell'energia elettrica, acquedotti e così via. Uno sviluppo interessante in questo campo è la potenzialità di creare computer embedded "intelligenti" che sfruttano i vantaggi del "fog computing". In breve, su un singolo server non sarà mai disponibile un file completo, ma il file stesso sarà "disperso" in pacchetti su diversi server. Quindi solo un utente autorizzato avrà il know-how necessario per riassemblare i diversi pacchetti dispersi per ricreare il file completo.
Anche se IoT (Internet of Things) si è da tempo affermata nell'ambito consumer, stanno incominciando a emergere interessanti opportunità nel campo industriale e ciò farà da traino a un'altra tendenza che si sta facendo strada nel campo dell'elaborazione embedded: il passaggio dalle architetture Plc a quelle Pc, stimolato dalla massiccia adozione di macchinari della prossima generazione che richiedono più "intelligenza" e flessibilità rispetto a quelle che un tradizionale Plc è in grado di fornire.
Uno dei principali vantaggi legati all'utilizzo dei Pc per il controllo industriale è rappresentato dal fatto che essi contribuiscono a superare le problematiche legate all'obsolescenza di macchinari e apparecchiature "smart", oltre a consentire una gestione più flessibile dei requisiti di I/O presenti e futuri utilizzando tecniche come ad esempio la virtualizzazione. Per questo motivo Intel ha deciso di estendere il periodo di disponibilità dei processori destinati al mondo industriale, dai 7 anni attuali a 15 anni, raddoppiando la longevità di alcuni dei suoi attuali prodotti. I processori Atom della serie E3800 di Intel, ad esempio, sono i primi micro per i quali è prevista una disponibilità per tre lustri, con tutti i vantaggi che ciò comporta per le aziende produttrici.

Filippo Fossati
filippo.fossati@fieramilanomedia.it

I sistemi di visione embedded, dalla complessità alla semplicità

Se per l'essere umano vedere è un processo intuitivo, per le macchine "vedere" è estremamente complicato. Le tecnologie di visione integrata aiutano i sistemi a "vedere", estraendo dalle immagini acquisite le informazioni necessarie. Si tratta di una sfida enorme ma le giuste soluzioni possono trasformare un compito di complessità scoraggiante in un processo all'insegna della semplicità. I numerosi miglioramenti ottenuti dalle nuove tecnologie di elaborazione delle immagini - dal consumo energetico alla qualità dei sensori, dalle prestazioni agli algoritmi di elaborazione, fino all'apprendimento automatico – hanno permesso alla visione artificiale di raggiungere livelli solo poco tempo fa inimmaginabili

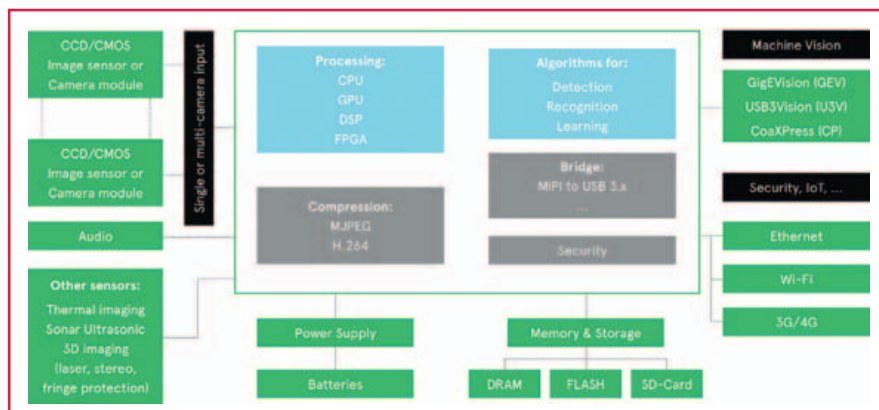
Michael Uyttersprot
Technical Marketing Manager
Avnet Silica

La combinazione tra sistemi embedded e sistemi di visione artificiale ha dato vita a un'area di mercato completamente nuova: quella dei sistemi di visione embedded. La visione embedded offre tutte le potenzialità per creare valore in quasi tutti i settori applicativi dell'elettronica. Grazie ai rapidi sviluppi e ai continui miglioramenti di hardware e software, in un futuro prossimo si può già immaginare una rapida proliferazione di queste tecnologie. I prodotti dotati di capacità di visione si affermeranno in moltissime applicazioni consumer, automobilistiche, industriali, sanitarie e domotiche.

Trasformazione e interazione

Internet of Things (IoT) sta trasformando profondamente l'industria elettronica, Questo paradigma renderà i dispositivi sempre più intelligenti e accessibili, permettendo loro di interagire con gli utilizzatori ovunque si trovino nel mondo. Solitamente i dispositivi sono molto più utili se, oltre a semplificare la nostra vita, sono in grado di interfacciarsi con il mondo fisico. Sotto questo aspetto la visione gioca un ruolo importante: essa consente di acquisire una mole immensa di informazioni indispensabili per l'interazione con l'ambiente fisico circostante. Un esempio classico è l'automazione, uno dei primi e dei principali settori applicativi dei sensori di immagine. Nella robotica, ad esempio, i sensori di immagine rappresentano gli "occhi" del sistema e contribuiscono ad azionare i motori in modo efficiente. Sempre nel settore dell'automazione, i recenti sviluppi nel campo dell'apprendimento auto-

Fig. 1 – Un tipico sistema di visione embedded di fascia alta

matico basato su reti neurali convoluzionali, CNN, e su altre reti neurali, permettono di usufruire di sistemi di visione intelligenti dotati di autoapprendimento.

Le nuove sfide

Lo sviluppo delle applicazioni di visione embedded comporta molte sfide che coinvolgono ogni parte del sistema. Applicata al quotidiano, la visione embedded è pensata per operare in contesti in cui parametri e condizioni - per esempio i livelli di illuminazione, il movimento o l'orientamento - cambiano costantemente. In tale contesto, l'impiego di speciali algoritmi di visione per controllare i dati è essenziale. Fare affidamento sulle sole simulazioni non è sufficiente; occorrono test effettuati nel mondo reale.
Tali verifiche possono richiedere molto tempo.
Ciò vale soprattutto nelle applicazioni legate al settore automotive, alla robotica e alla sicurezza.
Altro elemento importante è il trattamento dei dati. A seconda della qualità delle informazioni grezze acquisite – dai video alle immagini fisse – possono rendersi necessari importanti interventi di ottimizzazione ed elaborazione. Un esempio è quello di una lente di qualità insufficiente il cui output, se non adeguatamente compensato, potrebbe compromettere l'intero sistema di elaborazione delle immagini.

Avnet Silica & Xilinx

Guida autonoma, robot chirurgici e fabbriche automatizzate sono solo alcuni esempi delle ultime innovazioni che dipendono dalla sofisticata tecnologia di visione integrata. Sebbene l'elaborazione delle immagini sia sempre stato un terreno colonizzato dal software, i SoC dotati di logica programmabile hanno spostato l'ago della bilancia. I colli di bottiglia a livello software possono essere rimossi grazie alla logica programmabile ad alte prestazioni, pur mantenendo la riconfigurabilità necessaria per un rapido aggiornamento. La programmabilità permette inoltre di semplificare la personalizzazione, consentendo di indirizzare qualsiasi applicazione di visione integrata che potrebbe emergere nel mercato. Dotare le macchine della capacità di vedere, percepire e rispondere immediatamente agli stimoli dell'ambiente circostante crea enormi opportunità in termini di differenziazione. Tuttavia, questo comporta diverse sfide in termini di prestazioni, ambienti di programmazione e cicli di progettazione, implicando per i progettisti l'esigenza di creare e lanciare sul mercato architetture di nuova generazione. Per superare le sfide legate alla visione integrata, Avnet Silica e Xilinx sono congiuntamente impegnate a offrire kit di progettazione e progetti di riferimento che hanno l'obiettivo di ridurre la complessità software e hardware. La natura programmabile degli strumenti proposti riduce la complessità dello sviluppo portandola al livello dei progetti basati su processore. Con un ambiente di programmazione più semplice, è possibile lavorare sul software e quindi ottimizzare l'hardware attorno a una soluzione. Un altro elemento che scaturisce della proposta congiunta riguarda i volumi d'ordine: indipendentemente dalle quantità, Avnet Silica e Xilinx possono lavorare insieme per supportare qualsiasi esigenza. Grazie all'approccio programmabile è possibile creare prodotti flessibili e scalabili e con kit e strumenti che integrano funzionalità chiave, è possibile semplificare il ciclo di sviluppo e ridurre la curva di apprendimento. Il supporto per sensori, connettività wireless, memoria, fotocamere, connettori cloud e catene per segnali analogici e RF, permette l'integrazione con qualsiasi piattaforma, consentendo di ottenere le migliori soluzioni.

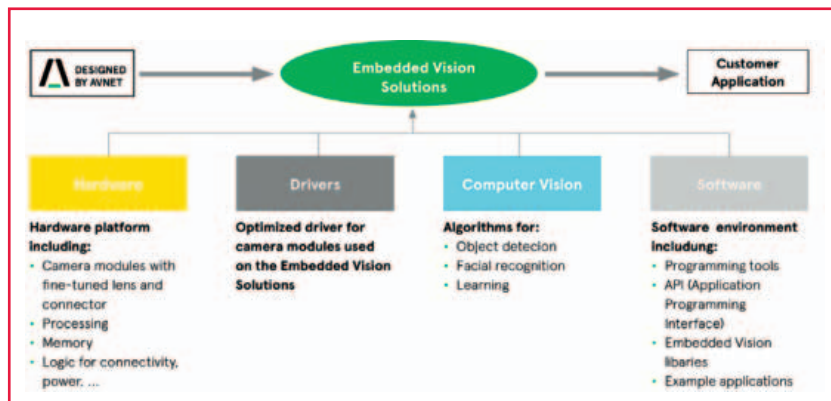



Fig. 2 – Soluzioni di visione embedded

Altro esempio è quello delle applicazioni legate alle immagini ad alta definizione, dove l'acquisizione e gestione di enormi quantità di dati in tempo reale richiede potenti sistemi di elaborazione parallela o circuiti hardware dedicati come GPU, DSP, FPGA o coprocessori. Spesso, però, i sistemi di visione embedded devono sottostare a vincoli stringenti di costo, dimensioni e consumi energetici. Può succedere, quindi, che un motore di elaborazione di fascia alta - dotato della necessaria potenza di calcolo - possa rivelarsi troppo costoso o troppo avido di energia per l'applicazione cui è destinato. Tutte queste esigenze vanno quindi attentamente bilanciate, ma spesso l'equazione non è così semplice da risolvere.

I componenti di sistema

I sistemi di visione embedded includono un'ampia gamma di componenti. La loro integrazione può seguire percorsi differenti ma soprattutto deve tenere conto della eterogeneità delle tecnologie utilizzate per effettuare l'acquisizione dell'immagine e la sua elaborazione. A tale proposito è essenziale selezionare gli elementi giusti in funzione delle esigenze del sistema e dell'applicazione, procedendo poi ad una regolazione fine dei vari componenti: hardware, software e algoritmi. Un compito non sempre facile. La complessità delle applicazioni di visione embedded rende indispensabile per gli sviluppatori l'uso di strumenti professionali capaci di ridurre costi, tempi e rischi di sviluppo, senza dimenticare il time to market dei progetti (Fig. 1). Per quanto riguarda l'input del sistema, i sensori in tecnologia CMOS e CCD (Charge-Coupled Device) rappresentano le due principali soluzioni oggi disponibili per acquisire l'immagine. I CCD offrono una qualità complessivamente più alta ma, nell'ultimo decennio, i miglioramenti delle tecnologie CMOS hanno permesso di colmare il divario. Oltre a permettere di gestire condizioni di bassa illuminazione, i sensori CMOS offrono oggi una migliore qualità di immagine, minori consumi energetici e un costo più contenuto. La loro diffusione, pertanto, è notevolmente superiore rispetto ai CCD. La tecnologia CMOS continua ad evolversi. Le direttrici di sviluppo riguardano la riduzione della dimensione dei pixel e l'implementazione di interconnessioni ad alta velocità e a banda più larga. I sensori di immagine di nuova generazione sono inoltre alloggiati in package e moduli sempre meno ingombranti che offrono la possibilità di realizzare - per esempio - soluzioni compatte a doppia telecamera per implementazioni di visione stereoscopica che consentono di compensare le distorsioni, di rilevare la profondità, e di migliorare le caratteristiche di gamma dinamica e nitidezza.

Dotazioni specifiche

Per la scelta del processore di un sistema di visione occorre considerare aspetti quali le prestazioni in tempo reale, il consumo di energia, la qualità dell'immagine e la complessità dell'algoritmo. Ai continui miglioramenti in merito alla potenza di elaborazione e agli algoritmi di visione, si affiancano aspetti quali una maggiore integrazione con le soluzioni SLAM (simultaneous localisation and mapping) concepite per le applicazioni automobilistiche, la robotica e i droni. Un requisito sempre più importante dei sistemi di visione è anche una crescente e cospicua dotazione di memoria locale, volatile e non volatile, indispensabile per consentire di confrontare grosse moli di immagini o di conservarne i dati in attesa dell'analisi. Un altro elemento essenziale del sistema sono gli algoritmi specializzati per le applicazioni di visione, ad esempio per controllare le immagini video in ingresso ed effettuare elaborazioni mirate tipicamente al miglioramento dei colori o al rilevamento di oggetti. Dopo la crea-

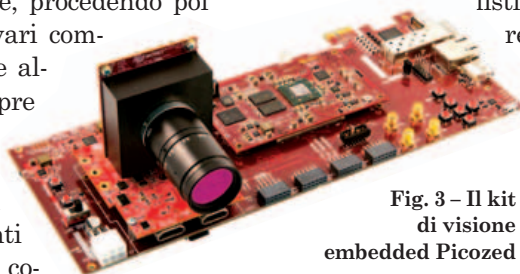



Fig. 3 – Il kit di visione embedded Picozed

zione della libreria di visione artificiale open-source OpenCV, il processo di sviluppo e implementazione degli algoritmi è cambiato drasticamente. Grazie al codice di programmazione e alle funzioni C/C++ centrate sulle applicazioni di visione, OpenCV facilita il trasferimento e l'esecuzione degli algoritmi sui processori embedded. Sono molte le aziende che offrono soluzioni di visione e di elaborazione video basate su OpenCV (o su librerie simili, e perfino su framework), per una varietà di applicazioni. Generalmente anche i produttori di semiconduttori offrono librerie dedicate alla visione artificiale che hanno l'obiettivo di potenziare le soluzioni di elaborazione basate sui loro prodotti. Infine, un ulteriore elemento che sta acquisendo una crescente importanza soprattutto alla luce dell'avvento delle soluzioni IoT è la connettività, sia essa di tipo cablato o wireless a seconda dell'applicazione e dei suoi requisiti. In quest'ottica l'importanza della connessione è ulteriormente accentuata dall'avvento di software in grado di eseguire analisi algoritmiche a livello di server nel cloud.

Figure 3bis – Kit Kinetis-NXP

Soluzioni complete

Avnet Silica vanta una grande esperienza nel supportare i clienti nello sviluppo di applicazioni di visione embedded. La società offre letteralmente tutti i blocchi costruttivi necessari per dare vita a un sistema di visione embedded completo, con un portafoglio di soluzioni hardware e software ottimizzate, di driver e di applicazioni. La gamma dei blocchi disponibili spazia dai sensori di immagine ai moduli telecamera, arrivando fino a componenti hardware dedicati, come processori, memorie e unità di alimentazione in grado di soddisfare i requisiti più critici di elaborazione e consumo energetico. A questi blocchi si affiancano strumenti di sviluppo, driver per telecamere, progetti di applicativi di riferimento e un grande know-how nel campo del software e degli algoritmi di elaborazione delle immagini (Fig. 2). Oltre a fornire assistenza nello sviluppo di soluzioni full-custom per aiutare i clienti a realizzare le proprie piattaforme e i propri prodotti di visione embedded, Avnet Silica ha al proprio attivo anche un'ampia gamma di proposte avanzate pronte all'uso per la realizzazione di telecamere e molto altro ancora. Un esempio è il kit di visione embedded PicoZed, costruito utilizzando l'omonimo system-on-module (SoM), il quale a sua volta si basa sul system-on-chip (SoC) programmabile Xilinx Zynq-7000. Il kit PicoZed è ideale per le applicazioni di visione artificiale e comprende tutti i componenti hardware, software e IP necessari per lo sviluppo di applicazioni video personalizzate. La soluzione supporta inoltre reVISION, by Xilinx, uno stack di accelerazione riconfigurabile ottimizzato per applicazioni di visione artificiale e di apprendimento automatico guidato da visione. Lo stack comprende risorse per lo sviluppo della piattaforma, dell'algoritmo e dell'applicazione; offre funzioni OpenCV accelerate a livello hardware e supporta le reti neurali più diffuse. Un secondo esempio è il kit di sviluppo per telecamere STM32F7 di Avnet Silica. Economico e compatibile con Mbed, offre basso assorbimento di corrente, un'interfaccia USB, un display tattile capacitivo a colori di 4,3 pollici e tutto l'hardware e il software necessario per il rapido sviluppo di soluzioni di visione embedded rivolte ad Internet of Things (IoT), domotica e altre applicazioni video. Una terza possibilità è il kit Kinetis, a basso consumo, basato sul microcontrollore NXP Kinetis K82F Cortex-M4. Il kit comprende un modulo telecamera VGA miniaturizzato con connettore flessibile, una lente con campo visivo orizzontale di 90 gradi e un filtro IR, ed è in grado di acquisire immagini fisse o di generare un flusso video a bassa risoluzione in tempo reale (Fig. 3). Avnet Silica continua ad ampliare la propria gamma di kit pronti all'uso con l'aggiunta di nuovi prodotti, proponendo ai clienti un'ampia scelta di soluzioni avanzate per la visione embedded.

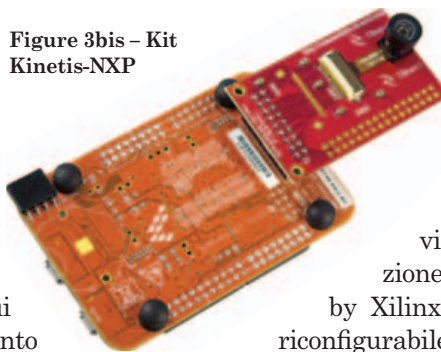
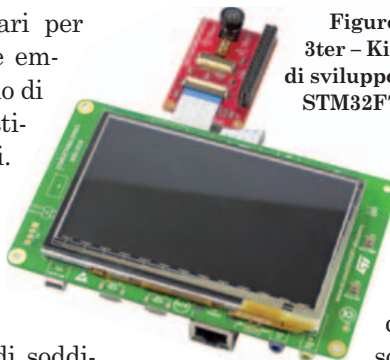
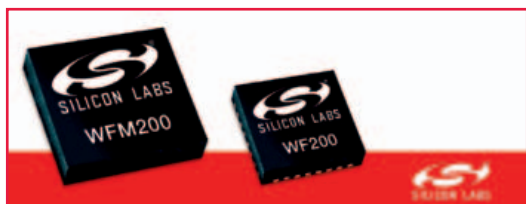



Figure 3ter – Kit di sviluppo STM32F7

Ulteriori informazioni sulle soluzioni Avnet Silica per la visione embedded sono disponibili a: https://www.avnet.com/wps/portal/silica/solutions/markets/embedded-vision

I nuovi dispositivi Wi-Fi di Silicon Labs per applicazioni IoT

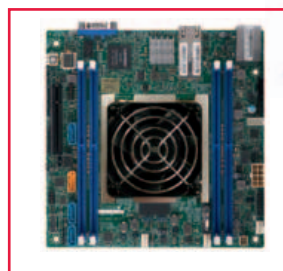
Francesco Ferrari

I nuovi prodotti Wi-Fi di Silicon Labs sono stati progettati per semplificare i progetti di applicazioni a basso consumo alimentati a batteria

Silicon Labs ha annunciato l'introduzione di una nuova serie di prodotti Wi-Fi ottimizzati dal punto di vista dei consumi energetici. Si tratta dei transceiver WF200 e dei moduli WFM200 che supportano trasmissioni in modalità Wi-Fi nella banda dei 2,4 GHZ con i protocolli 802.11 b/g/n. L'introduzione di questi nuovi componenti ha come obiettivo la semplificazione dei progetti di prodotti a basso consumo alimentati a batteria che utilizzano la tecnologia Wi-Fi come per esempio telecamere di sicurezza IP, terminali PoS (Point of Sale) e prodotti consumer per l'assistenza sanitaria. In sostanza si tratta di una serie di prodotti Wi-Fi a basso consumo espressamente concepiti per le applicazioni IoT, visto anche l'incremento delle richieste da parte del mercato di componenti in grado di rispettare i vincoli in termini di ingombri e di consumi imposti dai dispositivi alimentati a batteria. Il ricorso al modulo WFM200, particolarmente compatto grazie anche al package SiP (System-in-Package) con antenna integrata, permette, inoltre, di ridurre il time-to-market per la realizzazione di prodotti Wi-Fi miniaturizzati alimentati a batteria. Il transceiver WF200, invece, si posiziona come opzione economica per le applicazioni in alti volumi e consente ai progettisti di soddisfare requisiti specifici come per esempio il ricorso a antenne esterne. I nuovi prodotti di Silicon Labs offrono diversi vantaggi per le applicazioni IoT che utilizzano la tecnologia Wi-Fi. Per esempio, la potenza utilizzata in trasmissione e in ricezione è particolarmente contenuta (sono richiesti rispettivamente 138 mA e 48 mA). Sempre per ridurre i consumi a livello di sistema, il consumo medio del Wi-Fi è pari a 200 µA (DTIM = 3) mentre per le trasmissioni Wi-Fi su lunga distanza il Link budget (bilancio di collegamento) è di 115 dBm.Silicon Labs ha curato anche la diversità spaziale e di coesistenza wireless in ambienti dove sono presenti altri dispositivi che utilizzano la banda a 2,4 GHz. Per quanto riguarda la miniaturizzazione, il transceiver è ospitato in un package di tipo QFN32 che misura 4 x 4 mm, mentre il modulo è disponibile in package SiP LGA52 (le misure sono di 6,5 x 6,5 mm), entrambe soluzioni particolarmente interessanti per applicazioni dove lo spazio è limitato. Non mancano le tecnologie per la sicurezza come per esempio l'accelerazione hardware degli algoritmi di cifratura che supporta gli standard AES, PKE e TRNG, protezione dell'interfaccia verso l'host e boot sicuro.Gli sviluppatori possono ridurre i tempi di sviluppo, le risorse impiegate e i rischi grazie alla pre-certificazione di conformità con le direttive FCC, CE, IC mentre per quanto riguarda la disponibilità di appositi tool ci sono numerose opzioni come per esempio uno starter kit per applicazioni wireless che comprende driver per host Linux ed embedded. La produzione in volumi è prevista per il quarto trimestre di quest'anno.

Le novità di Supermicro per l'embedded

Francesco Ferrari

Supermicro ha realizzato per il settore embedded nuove soluzioni basate sui recenti SoC Intel Xeon D-2100 (quelli con il nome in codice Skylake-D) e Atom C3000. Le schede madri X11SDV offrono funzionalità RAS (reliability, availability, serviceability) tipiche dei prodotti per server per applicazioni di elaborazioni a livello edge. Si tratta di soluzioni bilanciate e ottimizzate, caratterizzate da un ciclo di vita particolarmente lungo, che mettono a disposizione degli sviluppatori fino a 18 core per l'elaborazione, un massimo di 512 GB di memoria DDR4 a quattro canali che opera a 2.666 MHz, fino a quattro por-

te 10 GbE con supporto RDMA e disponibili con un engine di accelerazione integrato Intel QAT (Quick Assist Technology) per la cifratura. A queste funzionalità si aggiungono anche quelle per lo storage mini-PCIe, M.2 e NVMe. Supermicro ha presentato anche una compatta soluzione fanless basata sui processori Atom Low Power, e una soluzione modulare, sempre fanless, in grado di operare in condizioni estreme dal punto di vista della temperatura, con protezione da polvere e condensa certificata IP51.

La motherboard X11SDV di Supermicro offre funzionalità di livello server in una soluzione particolarmente compatta

Harwin: connettori board-to-board per elevate densità di stacking

Emanuele Dal Lago

La serie di connettori Archer Kontrol di Harwin sono stati rpogettati per rispondere a una vasta gamma di esigenze in ambito industriale

Harwin ha annunciato l'introduzione di una nuova famiglia di connettori board-to-board che mette a disposizione dei progettisti soluzioni di connessione particolarmente affidabili, ma comunque flessibili, in grado di soddisfare una vasta gamma di esigenze in ambito industriale. La nuova serie si chiama Archer Kontrol e i connettori sono disponibili in versioni con un numero di pin compreso tra 12 e 80. Il passo utilizzato è quello a 1,27 mm e i contatti possono supportare correnti nominali fino a 1,2 A. Harwin realizza versioni sia con orientamento sia orizzontale che verticale. Nei modelli con orientamento verticale sono previste opzioni con altezze differenti. Per le principali caratteristiche tecniche, i connettori hanno un resistenza di isolamento pari a 1.000 MΩ (min.), tensione nominale di 500 VAC e intervallo di temperatura di funzionamento compresa tra -55 °C e 125 °C. Le specifiche di questi connettori prevedono il supporto per un minimo di 500 cicli di accoppiamento/disaccoppiamento. Per quanto riguarda l'assemblaggio, questi connettori sono predisposti per i sistemi a montaggio superficiale in modo da semplificare i processi di produzione automatici, mentre le apposite ritenzioni assicurano la stabilità del fissaggio sulla scheda PCB. I contatti in bronzo fosforoso di questi connettori hanno aree di contatto placcate in oro per migliorare la saldabilità. I dispositivi della serie Archer Kontrol di Harwin sono forniti in confezione nastrata (tape&reel), con cappucci sui connettori in configurazione verticale per semplificare le operazioni di pick&place nella produzione automatizzata. L'alloggiamento di questi connettori è stampato in un materiale LCP resistente alle alte temperature in conformità alle specifiche UL94V-0. Lo specifico design dei connettori Archer Kontrol è stato concepito anche per incrementare la resistenza dei connettori alle forze laterali e di torsione che possono essere presenti in applicazioni dove sono previste vibrazioni. I connettori sono completamente protetti e polarizzati fornendo un aiuto in caso di connessione con accoppiamento cieco, e sono in grado di sopportare disallineamenti di notevole entità. La famiglia prevede configurazioni board-to-board parallela oppure motherboard-to-daughterboard ad angolo retto compatibili con le tipologie di connettori standard più diffuse (in questo modo si semplifica la sostituzione). Dal punto di vista delle possibilità di impiego, la disponibilità di modelli con diverse altezze e combinazioni di pin permette di usare questi nuovi connettori per applicazioni che prevedono lo stacking di più schede. Le possibili applicazioni sono numerose e comprendono, per esempio, i controlli e azionamenti industriali, oltre ai numerosi dispositivi hardware utilizzati all'interno degli stabilimenti, sistemi di acquisizione dati, installazioni IoT, strumentazione di monitoraggio portatile, apparecchiature per uso ferroviario, sistemi di controllo dei veicoli, apparati di telemetria e di monitoraggio installate lungo strade e ferrovie.

Investimenti IoT: metterli a frutto usando (bene) i Big Data

Ricavare valore di business dalle enormi moli di informazioni generate da impianti e oggetti "smart" significa rendere accessibili tutte le fonti dati, usando, in funzione dell'applicazione, i corretti strumenti analitici

Giorgio Fusari

Solo qualche anno fa "Internet of Things", o IoT, sarebbe risultato un termine sconosciuto o incomprensibile ai più: oggi sta diventando un paradigma fondante per realizzare modelli di automazione come Industria 4.0, e sofisticate tecniche di produzione, improntate sullo "smart manufacturing". L'obiettivo di chi decide di investire per realizzare un'applicazione IoT è sempre lo stesso: aumentare, grazie a una maggior "intelligenza" delle macchine e dei processi, l'efficienza degli impianti industriali e aziendali, migliorare la competitività, creare nuovi tipi di servizi e accrescere la soddisfazione degli utenti finali. Tra questo obiettivo e il suo reale raggiungimento ci sono però ancora di mezzo diversi punti critici da affrontare e superare. E un elemento, certo discriminante, per giustificare l'investimento in una data applicazione IoT è verificare se poi le grandi moli di dati che genera, e consente di raccogliere, sono davvero così utili a migliorare l'attività di business. Poter rispondere positivamente a questa domanda dipende molto dall'approccio tecnologico e architetturale adottato nella raccolta, successiva analisi e interpretazione, delle grandi quantità di dati che sensori, tag RFID (radio frequency identification), contatori intelligenti, dispositivi e oggetti "smart" disseminati in impianti industriali, apparecchiature e prodotti, registrano di continuo.

Cresce la velocità, e si va oltre Hadoop

La velocità diventa sempre più un requisito chiave nell'analisi dei Big Data, e l'esigenza di rapidità sta guidando l'adozione di database più veloci come Exasol e MemSQL, di data store "Hadoop-based" come Apache Kudu, e tecnologie che consentono di eseguire query più rapide. Questa è una delle tendenze chiave prevista in un rapporto, stilato da Tableau Software, sui dieci top trend per i Big Data. Per inciso, Tableau, assieme a Microsoft, figura nella posizione di punta del Magic Quadrant per la business intelligence (BI) e gli "analytics", elaborato da Gartner per l'anno in corso. Gli acceleratori di query, sottolinea Tableau, utilizzando motori SQL-on-Hadoop (Apache Impala, Hive LLAP, Presto, Phoenix, Drill) e tecnologie OLAP-on-Hadoop (AtScale, Jethro Data, Kyvos Insights), stanno poi ulteriormente offuscando le linee di demarcazione tra warehouse tradizionali e mondo dei grandi dati. Secondo top trend: se negli ultimi anni, sull'onda dei Big Data, sono emerse varie tecnologie per soddisfare l'esigenza di tool analitici basati sulla piattaforma Hadoop, ora tali tool diventano obsoleti, a favore di tecnologie e piattaforme agnostiche rispetto ai dati e alle fonti, e in grado di soddisfare la domanda e i casi d'uso dei vari utenti aziendali. Soprattutto le imprese con ambienti IT eterogenei e complessi, con dati "seppelliti" in una molteplicità di fonti (basi dati tradizionali, sistemi di data warehousing cloud-

Fig. 1 – L'analisi intelligente dei Big Data permette d'incrementare non solo l'efficacia degli impianti, ma anche l'efficienza energetica di macchine e sistemi (Fonte: Siemens)

based, dati strutturati e non strutturati provenienti da fonti Hadoop e non-Hadoop) non puntano più, per le applicazioni di BI, su un approccio di tipo "a silos" focalizzato su un'unica sorgente di dati (Hadoop), ma richiedono funzionalità analitiche in grado di agire su tutte le tipologie di fonti e informazioni disponibili. Terzo trend su cui porre attenzione: le imprese non si limiteranno più, semplicemente, a riempire di informazioni i loro "data lake", ma cercheranno di farne un uso agile e ripetibile per ottenere risposte rapide ai propri problemi di business, valutando attentamente i vantaggi ottenibili, prima di investire personale e infrastrutture in tale area. Tra gli altri trend, la progettazione delle architetture si fa più specifica, per incontrare le precise esigenze di analisi dei dati di ogni singolo settore; la varietà dei dati, e non il loro volume o velocità, guida in prospettiva gli investimenti sui Big Data; Apache Spark diventa la piattaforma di elezione per le imprese, e l'abilità dei computer di analizzare grandi quantità di informazioni con efficienza porta in primo piano l'intelligenza artificiale (AI) e le tecnologie e algoritmi di apprendimento automatico (machine learning - ML). Cresce la domanda di tool analitici in grado di connettere e combinare un'ampia varietà di fonti dati ospitate nel cloud, per riuscire a esplorare e visualizzare ogni tipo di informazione, indipendentemente dal sistema in cui è memorizzata. Inoltre, l'emergere delle piattaforme analitiche "self-service", che rendono più facilmente accessibili i dati di Hadoop agli utenti aziendali e ai professionisti delle LOB (line of business), sta facendo diventare di ampia diffusione anche i tool self-service (come Alteryx, Trifacta, Paxata) che permettono di ridurre ulteriormente il tempo e la complessità di preparazione dei dati per la successiva analisi, soprattutto quando si ha a che fare con una varietà di tipologie di dati e formati.

Fig. 2 – Fonte: Pixabay

Internet of Things e Big Data

In questi anni, l'emergere e il crescente sviluppo della Internet of Things ha portato a dover inserire nella categoria Big Data anche tutte le enormi moli di dati acquisiti, scambiati, elaborati e gene-

"Grandi dati", la terminologia

Espressione spesso abusata, specie nelle comunicazioni con precipui obiettivi di marketing, il termine "Big Data" viene utilizzato da tecnici e addetti del settore per indicare volumi di dati molto grandi, suddivisibili in due principali categorie di informazioni: quelle di tipo strutturato, generate dalle interazioni umane attraverso i processi di business esistenti tra le varie organizzazioni - quindi i dati, organizzati in campi e record, all'interno dei classici database (anagrafiche clienti, ordini vendite, transazioni di pagamento) - e quelle di tipo destrutturato, o non strutturato. Queste ultime si chiamano così perché non si trovano memorizzate in database o altre strutture dati, ma sono informazioni generate da attività umane legate all'uso della tecnologia digitale, come posta elettronica, sistemi di messaggistica, videoscrittura, applicazioni multimediali. Come tali, queste informazioni possono dunque essere costituite da file testuali, file audio, file video. In verità, oltre ai dati strutturati e non strutturati, esiste anche una terza categoria, "intermedia" rispetto alle prime due, quella dei dati semi-strutturati. Tali informazioni non sono organizzate in strutture dati indirizzabili e analizzabili in modo sofisticato, ma possono avere un dato associato che le rende reperibili. Ad esempio, un documento prodotto con un sistema di videoscrittura è considerato di norma un dato non strutturato, tuttavia, nel momento in cui ad esso viene aggiunto un tag, una parola chiave, quindi un metadato che ne rappresenta il contenuto rendendolo più facile da ritrovare nelle ricerche, questo diventa un dato semi-strutturato.

Fig. 3 – Fonte Pixabay

rati in modo automatico dalle macchine nelle più svariate applicazioni embedded M2M (machine-to-machine) e IIoT (Industrial Internet of Things) di ultima generazione. A seconda dei dispositivi e delle modalità di acquisizione (reti di sensori, tag RFID, file di registro di computer, log di rete, telecamere di videosorveglianza, e quant'altro) questi Big Data possono essere di tipo strutturato, non strutturato, semi-strutturato (vedi box "Grandi dati", la terminologia). Vi sono però altre importanti caratteristiche che identificano i Big Data: la società di ricerche Gartner li definisce come dati di elevato volume, elevata velocità, e/o elevata varietà, che necessitano di efficienti e innovative forme di elaborazione delle informazioni, per abilitare migliori intuizioni, prese decisionali e automazione di processo. In ragione di tutte le caratteristiche sopra descritte, in sostanza, i Big Data non sono più gestibili, sia in fase di raccolta, sia in fase di analisi ed elaborazione, attraverso le tecnologie e i database tradizionali. Ciò perché questi dati vanno non solo raccolti in grande quantità, ma devono anche essere analizzati ed elaborati con notevole efficienza, e, sempre più, in tempo reale, per riuscire a innovare un processo, un prodotto, un servizio, e produrre un effetto positivo il più possibile immediato sulla conduzione del business.

Architetture di elaborazione

Il volume, la varietà, la disomogeneità dei Big Data, e la loro provenienza da fonti disparate, complicano i processi di raccolta, analisi, elaborazione dei dati, per l'estrazione (mining) di "insights" e conoscenze subito utilizzabili. In fase di raccolta delle informazioni, gli strumenti analitici devono avere la capacità di accedere ed esplorare i dati di tutte le fonti e formati importanti per l'applicazione da realizzare, a prescindere dal fatto che questi si trovino memorizzati in database convenzionali, data warehouse, file system distribuiti, sistemi Hadoop o repository ospitati nel cloud. Allo stesso modo, devono risultare accessibili i dati acquisiti da tutte le attrezzature, device e apparati industriali, come possono essere i PLC (programmable logic controller), i sistemi SCADA (supervisory control and data acquisition), e i dispositivi IoT: sensori, gateway o altri device.
In fase di trasmissione, dover spedire ripetutamente grandi moli di dati grezzi ai motori analitici sui server nel cloud può rivelarsi molto costoso, oltre

Trasformare dati in conoscenza: le piattaforme IoT sul mercato

Lanciata da Siemens, ed ora in corso di espansione attraverso l'aggiunta di collaborazioni, interfacce e app, la piattaforma IoT "cloud-based" MindSphere è in grado di raccogliere e analizzare grandi volumi di dati di produzione, generando informazioni utili a migliorare l'efficienza degli impianti industriali. MindSphere viene fornita da Siemens nella modalità PaaS (Platform as a Service) e costituisce la fondazione per applicazioni e servizi forniti sia da Siemens stessa, sia da provider di terze parti, in aree come la manutenzione predittiva, la gestione dei dati energetici, l'ottimizzazione delle risorse. Siemens non è certo la sola nel settore, e l'offerta di piattaforme IoT che permettono agli utenti aziendali di sfruttare i Big Data per migliorare il proprio business continua ad arricchirsi: si va, ad esempio, dalla soluzione "end-to-end" Eurotech Everyware Device Cloud (EDC), a Microsoft Azure IoT Suite, che consente di connettere milioni di dispositivi e analizzare e visualizzare grandi quantità di dati operativi, anche in questo caso per sviluppare applicazioni come il monitoraggio remoto o la manutenzione predittiva. Ma si possono citare anche Bluemix, la piattaforma cloud di IBM che integra in un unico ambiente servizi d'infrastruttura e piattaforma con strumenti analitici e cognitivi; l'infrastruttura integrata Cisco UCS per i Big Data e gli analytics, o le soluzioni analitiche per i Big Data fornite dalla Google Cloud Platform.

che lento e dispendioso in termini di banda. Ciò è tanto più vero quando sensori, tag e dispositivi embedded IoT intelligenti che utilizzano connessioni wireless devono soddisfare determinati requisiti di velocità trasmissiva e consumare poca energia, per essere in grado di operare per lunghi periodi di tempo senza necessità di ricarica.
Problemi come questi stanno orientando la progettazione delle architetture IoT verso soluzioni in grado di eseguire almeno le funzioni di pre-elaborazione dati già a livello locale, trasmettendo ai motori di analisi nel cloud solo le informazioni rilevanti. Da questo punto di vista, in particolare, stanno acquistando importanza architetture che vengono definite di "fog computing" e "edge computing". Entrambe puntano a portare potenza e intelligenza di elaborazione più vicino a dove i dati vengono originati, quindi più vicino ai sensori e dispositivi che si trovano alla periferia della rete.

Fog computing e edge computing

Pur essendo spesso assimilate a un unico concetto, le architetture di fog computing e edge computing presentano differenze nel posizionamento dell'intelligenza e della potenza computazionale che viene aggiunta all'infrastruttura. Mentre nel fog computing tale intelligenza viene portata a livello della LAN (local area network), e integrata in nodi, appliance e gateway IoT, nel caso dell'edge computing, intelligenza e funzionalità di elaborazione sono aggiunte in zone ancora più periferiche dell'architettura di rete, integrandole direttamente in dispositivi come i PAC (programmable automation controller).
Elaborare, o pre-elaborare, i dati già a livello locale, nella periferia di rete, fornisce diversi vantaggi: non soltanto quello di risparmiare banda, ma anche l'opportunità di sfruttare sempre più in "tempo reale" le informazioni decisive per migliorare il business. Vanno poi aggiunti i benefici a livello di privacy, security e conformità con le normative di settore, derivanti dal fatto che i vari sensori, dispositivi ed endpoint non hanno necessità di trametterе di continuo verso il cloud, attraverso Internet, dati sensibili. Occorre tuttavia precisare che tali architetture di elaborazione distribuite continuano a conservare un ruolo complementare rispetto al cloud, di cui non possono sostituire le risorse di elaborazione, la potenza analitica e le funzionalità di machine learning.

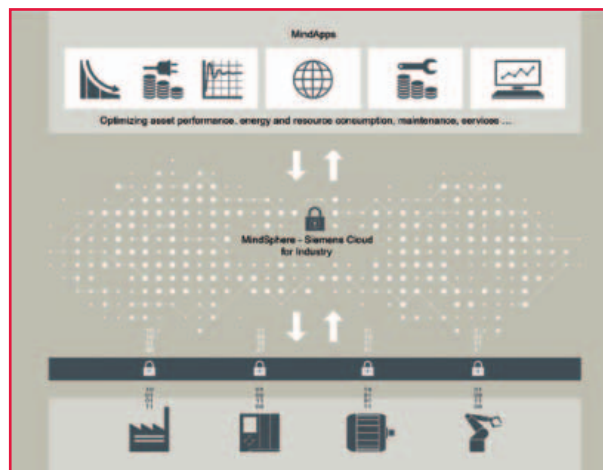



Fig. 4 – La piattaforma IoT "cloud-based" MindSphere di Siemens (Fonte: Siemens)

La fase di pre-elaborazione è necessaria a preparare i dati, prima dell'utilizzo vero e proprio all'interno dei modelli e algoritmi predittivi. In questa fase, in dati possono essere purificati da errori, duplicazioni, rumore del segnale; trasformati e ridotti a livello dimensionale, attraverso operazioni indirizzate a depurarli dalle informazioni ininfluenti dal punto di vista predittivo, e a individuare ed estrarre dati utili ad accrescere i risultati ottenibili dagli algoritmi di analisi nella fase successiva.
In quest'ultima, i dati pre-elaborati sono analizzati attraverso modelli predittivi, in grado di individuare schemi e far emergere informazioni preziose per il business. Qui, in funzione dei requisiti specifici dell'applicazione, occorre stabilire quando è conveniente applicare gli algoritmi analitici convenzionali, quindi classici modelli matematici ed equazioni, o diventa necessario utilizzare più sofisticati algoritmi di intelligenza artificiale e apprendimento automatico (machine learning).
Nel primo caso, l'implementazione del progetto può risultare più semplice, in quanto basata su algoritmi statistici e modelli predefiniti, meno avidi di risorse computazionali e più adattabili all'uso con i sistemi embedded. Nel secondo caso, si parla di algoritmi di machine learning, non più basati su equazioni o modelli predeterminati, ma in grado di apprendere, ed evolversi in maniera autonoma, in rapporto alle nuove informazioni elaborate. In sostanza, più dati analizzano, più i sistemi di machine learning riescono a identificare schemi nei dati, e a modificare e affinare l'algoritmo necessario per eseguire un determinato compito.

Starter Kit per progetti IoT

Sono gli elementi fondamentali per concepire le nuove reti IoT e verificarne il valore sul mercato e sono rivolti soprattutto ai maker delle start-up che sembrano più geniali in questa sfida

Lucio Pellizzari

Nel suo best-seller "**Crossing the Chasm**" del 1991 l'esperto di marketing high-tech **Geoffrey A. Moore** predicava che "crossing the chasm is hard for start-up". Tradotto letteralmente significa "attraversare il burrone è difficile per le start-up" ma è chiaro il concetto che già ventisei anni orsono per una giovane impresa di prodotti a elevato contenuto tecnologico era ben difficile fare carriera dato che anche qualora provasse a riuscirci veniva prontamente notata e assorbita da una società leader che l'acquisiva per poi chiuderla e incorporarne il know-how e (forse) i dipendenti. Se ciò avveniva quando IoT non esisteva, figuriamoci oggi che nascono continuamente giovani start-up spinte dalle buone idee che germogliano dall'ingegno dei tanti maker che si dilettano sulle soluzioni per IoT. Oggi per una start-up "crossing the chasm" non è più solamente difficile ma è proprio impossibile e, in effetti, in questa nuova forma di competizione imprenditoriale le start-up non mirano direttamente al proprio successo ma all'ambito premio di essere incorporate da una società leader che sappia accompagnare le loro idee al successo. D'altro canto, non si può negare che sono proprio le start-up a indovinare le idee di successo laddove i blasonati laboratori dei leader difettano di fantasia ed è perciò probabile che assisteremo ancora a lungo a questo susseguirsi di nascite e acquisizioni di start-up focalizzate ai prodotti e alle soluzioni per IoT. Nel frattempo diamo uno sguardo agli Starter Kit indispensabili ai maker e agli ingegneri per inventare le applicazioni IoT prossime venture.

Fig. 1 – Il CloudProfessor di Acer consente di realizzare reti IoT complete sui protocolli 802.11a/b/g/n ed è ideale per apprendere a creare codici direttamente da smartphone e tablet

Build Your Own Cloud

Acer ha reso disponibile lo Starter Kit CloudProfessor che offre ai maker e agli studenti una combinazione di risorse hardware e software insieme all'accesso ai servizi cloud Acer BYOC (Build Your Own Cloud). Questo set di componenti permette loro di realizzare reti IoT complete. Nel kit ci sono le schede di sviluppo Arduino Leonardo e LED101 e, inoltre, una base Arduino Shield Seeed, due LED, un sensore luminoso, un sensore termico e un azionamento motorizzato per i progetti robotici. A bordo troviamo una CPU Intel Atom x5-Z8300, una memoria Flash da 16 GByte, i front-end wireless 802.11a/b/g/n e il supporto delle schede microSD fino a 128 GByte. CloudProfessor può funzionare su smartphone e tablet compatibili con Android,

Chrome OS e iOS, supporta JavaScript e viene fornito con otto applicazioni pre-impostate.

ST e ARduino

Arduino e **STMicroelectronics** hanno realizzato Arduino STAR Otto con l'intento di offrire uno Starter Kit per la connettività Wi-Fi, Bluetooth e NFC e la possibilità di includere nei progetti anche prestazioni grafiche e audio di alta qualità attraverso

Fig. 2 – Arduino e STMicroelectronics presentano insieme Arduino STAR Otto pensato per progettare applicazioni IoT con connettività Wi-Fi, Bluetooth e NFC ed elevate prestazioni grafiche, audio e video

un display touch screen, una camera e una periferica Hi-Fi. Il microcontrollore è STM432F469BIT6 con core a 32 bit ARM Cortex M4 e clock di 180 MHz ed è accompagnato da 2 MByte di memoria Flash, 384 kByte di Sram, 16 MByte di Sdram e 128 kByte di Eeprom, con in più uno slot per memorie solide microSD. A bordo della scheda ci sono anche due microfoni MEMS2 di ST, un'interfaccia MIPI DSI e i front-end a 2,4 GHz con i supporti per Wi-Fi 802.11b/g/n. Il kit è provvisto di connettori per espansioni Arduino Uno, Due, Mega ed è compatibile con Arduino IDE.

IoT 3G e LTE

AT&T ha recentemente presentato il suo nuovo IoT Starter Kit 2.0 pensato per aiutare gli sviluppatori nei progetti che riguardano la molteplicità delle tecnologie cellulari 3G tipicamente legate ai costruttori di terminali mobili e ai fornitori di servizi mobili. Nel Kit c'è un modem WNC LTE Avnet M14A2A, una

Fig. 3 – Il nuovo IoT Starter Kit 2.0 di AT&T consente di sviluppare reti IoT connesse compatibili con la telefonia 3G e gestibili con le piattaforme cloud AT&T, IBM e Microsoft

NXP K64F Freedom Board compatibile con le schede Arduino e una SIM AT&T con 300 MByte di disponibilità dati per sei mesi. Il Kit è predisposto per lo sviluppo cloud con le piattaforme IoT AT&T M2X Data Service e Flow Designer ma può essere utilizzato anche con Microsoft Azure e IBM Bluemix.

Sensor-to-cloud

Avnet ha ulteriormente rinforzato la partnership con AT&T realizzando il nuovo Global LTE IoT Starter Kit composto dai due moduli Cellular IoT Starter Kit e LTE IoT Add-On Kit con cui si possono sviluppare applicazioni "sensor-to-cloud". Nel kit Avnet c'è l'AT&T IoT Platform Access con cui si possono utilizzare le piattaforme AT&T M2X e Flow Designer per lo sviluppo dei collegamenti machine-to-machine. Nella Development Board da 79,5x30 mm c'è un modem **WNC** M18QWG global LTE Cat-4 con cui configurare la connettività LTE e, inoltre, ci sono anche un sensore di luce ambientale, un sensore di temperatura e un accelerometro a tre assi. Per le espansioni c'è un connettore da 60 pin e un modulo Pmod da 2x6 pin.

Fig. 4 – Il nuovo Global LTE IoT Starter Kit Avnet per lo sviluppo delle applicazioni cloud sia IoT sia machine-to-machine sulle connessioni LTE

Wi-Fi 802.11b/g/n

GainSpan fa parte del gruppo **Telit** e ha introdotto la nuova GS2200M Starter Kit Board per favorire lo sviluppo delle applicazioni connesse. Nel kit c'è il modulo GS2200MIZ Ultra-low Power Wi-Fi 802.11b/g/n Mini-Module per la connettività wireless che misura 13,5x17,85x2,13 mm e garantisce consumi ultra ridotti a 260 nA in modalità "hibernate" e mediamente a 610 µA nell'elaborazione dei protocolli Wi-Fi, TCP, UCP e SSL. La CPU è ARM Cortex-M3 e a bordo ci sono le porte USB e Jtag per la programmazione e il debug, le interfacce di controllo Uart, SPI, SDIO e I2C e alcuni GPIO. La scheda ha i supporti compatibili con Arduino e Pmod e per l'alimentazione si accontenta di due pile AA.

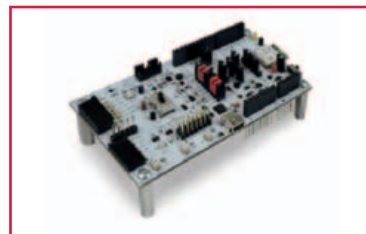



Fig. 5 – La GS2200M Starter Kit Board di GainSpan (Telit) permette di sviluppare le applicazioni cloud Wi-Fi 802.11b/g/n a consumo ultra-basso

IoT a corto raggio

Murata ha realizzato due Starter Kit passivi dedicati allo sviluppo delle applicazioni con gli RFIC **Nordic Semiconductor** nRF51 e nRF52. Sono supportati i protocolli wireless a corto raggio e a consumo ultra-basso Bluetooth Low Energy e ANT ma c'è un modulo a 2,4 GHz configurabile per protocolli proprietari come Gazell o NFC (Near Field Communication). Nel kit nRF51x22 troviamo l'RFIC Nordic nRF51, un front-end con i supporti a radiofrequenza e un cristallo insieme a tutti i componenti passivi necessari allo sviluppo dei nodi IoT wireless mentre nel kit nRF52x32 c'è anche un processore ARM Cortex-M4F con clock di 64 MHz e prestazioni di 215 Coremark e 58 Coremark/mA.

Fig. 6 – Con gli Starter Kit passivi Murata nRF51x22 e nRF52x32 si possono realizzare reti IoT wireless a corto raggio basate sugli RFIC Nordic Semiconductor

Gecko

Silicon Labs ha introdotto l'economico Starter Kit EFM32 Pearl Gecko PG12 SLSTK3402A utilizzabile per sviluppare applicazioni a consumo ultra basso con i microcontrollori Gecko Pearl PG12 e Jade JG12. I core sono ARM Cortex-M3 e Cor-

tex-M4 entrambi a 40 MHz e nella dotazione troviamo fino a 256 kByte di RAM, fino a 1024 kByte di Flash e motore crittografico AES-128/256, ECC, SHA1/2. Lo starter kit è composto da una scheda adatta a entrambe le CPU e una EFM32 Getting Starter Card con il software di base che consente fra l'altro di monitorare il consumo dal cavo USB o dalla batteria a bottone CR2032. A bordo ci sono anche un sensore di temperatura, un sensore di prossimità induttivo-capacitivo e un cristallo con LFXO di 32,768 kHz e HFXO di 40 MHz, oltre a uno zoccolo da 20 pin per un'eventuale espansione.

Fig. 7 – È per i microcontrollori Gecko Pearl PG12 e Jade JG12 il nuovo Starter Kit Silicon Labs SLSTK3402A che permette di sviluppare applicazioni a elevate prestazioni e consumo ultra-basso

IoT LoRaWAN

Sodaq ha realizzato con un finanziamento **Kickstarter** la scheda LoRaONE pensata per aiutare gli sviluppatori a progettare reti IoT **LoRaWAN** caratterizzate dalla velocità dati relativamente bassa e graduabile da 50 a 0,3 kbps grazie a cui riescono a supportare reti di oggetti IoT a consumi ultra bassi su distanze che possono superare una decina di chilometri. La scheda consente di progettare reti di sensori ideali da installare nelle metropoli e sono compatibili con le reti 3G/4G. LoRaONE è compatibile con Arduino, misura 40 x 25 mm e monta una MCU ATsamd21G18 a 32 bit con core ARM Cortex M0+ e clock di 48 MHz. A bordo troviamo 32 kByte di Sram, 256 kByte di Flash e 16 kByte di Eeprom, un front-end LoRa Microchip, un accelerometro/magnetometro ST LSM303D e 14 I/O.

Fig. 8 – La scheda LoRaONE di Sodaq permette di sviluppare reti di sensori IoT LoRaWAN con raggio d'azione di una decina di chilometri

IoT indossabili

Toshiba Electronics Europe ha presentato lo Starter Kit EBTZ1041-SK-A1 che consente di sviluppare applicazioni IoT indossabili usando il nuovo processore applicativo Toshiba TZ1041MBG. Il core è ARM Cortex-M4F a 32 bit ed è affiancato da 288 kByte di Sram e 1 MByte di Flash oltre che da un controller Bluetooth LE 4.1 che permette alla scheda di comunicare da e verso smartphone e tablet esterni utilizzabili per la configurazione delle funzionalità. A bordo c'è un transceiver Toshiba TC32306 che abilita la connettività wireless sub-GHz e c'è anche un connettore compatibile con Arduino UNO R3. La scheda permette di installare qualsiasi tipo di sensore e si possono pre-installare un accelerometro, un giroscopio o un magnetometro e anche algoritmi software specifici per pulsiossimetri o elettrocardiografi.

Fig. 9 – Per sviluppare applicazioni IoT indossabili Toshiba propone lo Starter Kit EBTZ1041-SK-A1 configurabile da smartphone con il supporto per sensori di ogni tipo

Riferimenti:

Acer http://home.cloud.acer.com/cpf/
Arduino www.arduino.org/products/boards/arduino-star-otto
AT&T http://starterkit.att.com/kits
Avnet www.avnet.com
GainSpan http://www.gainspan.com/products/gs2200m_skb
G. A. Moore http://www.geoffreyamoore.com/
Kickstarter www.kickstarter.com
LoRa Alliance www.lora-alliance.org
Murata www.murata.com
Nordic Semiconductor www.nordicsemi.com
Silicon Lab, www.silabs.com
Sodaq www.kickstarter.com/projects/sodaq/loraone-the-lora-iot-development-board/creator_bio
STMicroelectronics http://www.st.com/en/evaluation-tools/ard-otto-stm32.html
Telit www.telit.com
Toshiba https://toshiba.semicon-storage.com/eu/
Wistron NeWeb Corporation www.wnc.com.tw

Sensori sempre più intelligenti

La tecnologia dei sensori intelligenti riveste un elevato interesse in svariati settori applicativi, dai sistemi di controllo industriale all'automotive alle smart city e smart home, soprattutto con l'avvento dell'Industry 4.0 e dell'Internet of Things

Silvano Iacobucci

Uno degli avanzamenti più importanti nella tecnologia dei sensori negli ultimi dieci anni è stato lo sviluppo mirato di sensori intelligenti.
Un sensore è un dispositivo basato su un materiale le cui proprietà elettriche cambiano in funzione di un determinato fenomeno fisico, e che di conseguenza permette di trasformare una grandezza fisica (suono, vibrazione, temperatura, umidità, pressione, spostamento, accelerazione ecc.) in un segnale elettrico.
Il sensore si definisce intelligente ("smart sensor") quando contiene al suo interno anche un microcontrollore e tutta l'elettronica necessaria a effettuare direttamente alcune operazioni che in passato erano demandate a ulteriori sistemi centralizzati posti a valle: ad esempio pre-elaborare i valori delle misure effettuate, trasmettere tali valori attraverso segnali digitali e protocolli di comunicazione, effettuare in autonomia azioni di calibrazione e configurazione, prendere decisioni e attivare azioni in base a condizioni rilevate.
Il principale catalizzatore per la crescita della tecnologia dei sensori intelligenti è stato lo sviluppo della microelettronica a basso costo. Gli attuatori a chip per l'autocalibrazione e la compensazione meccanica possono essere creati utilizzando tecniche di micromachining o tecnologie a film sottile. Molte tecniche di fabbricazione del silicio vengono ora utilizzate per produrre anche sensori multistrato e array di sensori in grado di fornire una compensazione interna e aumentare l'affidabilità.
I sensori intelligenti consentono una raccolta più accurata e automatizzata dei dati in un' ampia varietà di ambienti, tra cui reti intelligenti, ricognizioni sul campo, esplorazione e diverse applicazioni scientifiche. Inoltre i materiali non lineari o dotati di isteresi, scartati fino ad oggi nella realizzazione di sen-

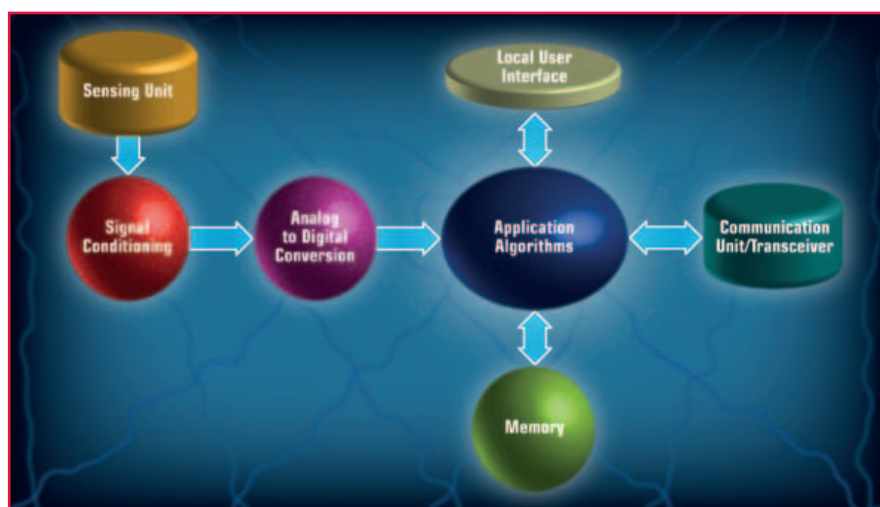



Fig. 1 – Principali componenti di un sensore intelligente

sori perché troppo inaffidabili o instabili per le applicazioni di rilevamento, possono ora essere applicati in un dispositivo smart in grado di effettuare tutte le compensazioni e pre-elaborazioni necessarie attraverso il microprocessore locale dedicato.

I sensori intelligenti offrono molteplici vantaggi, tra cui: minore manutenzione; ridotti tempi di downtime; maggiore affidabilità; tolleranza ai guasti; adattabilità per auto-calibrazione e compensazione; minore costo; minore peso; minori interconnessioni tra più sensori e sistemi di controllo; architetture di sistema meno complesse.

La figura 1 fornisce una rappresentazione schematica di un sensore intelligente dotato di un chip di elaborazione e trasmissione di segnale incorporato. I principali moduli componenti uno smart sensor comprendono: un elemento primario di rilevazione (l'unità "sensore" in senso stretto), un modulo di condizionamento del segnale (controllo di eccitazione, amplificazione a guadagno variabile, filtraggio analogico), un convertitore analogico-digitale, l'elaborazione digitale del segnale (algoritmi DSP) con relativa memoria e un modulo di comunicazione, oltre ovviamente a un sistema di alimentazione.

I sensori intelligenti consentono già oggi di realizzare processi industriali dinamici, ottimizzati in tempo reale e che si gestiscono autonomamente rendendo possibile lo sviluppo di una fabbrica intelligente Industry 4.0. Rilevano gli stati attuali del processo, li elaborano in dati digitali e li mettono a disposizione in tempo reale. Gli smart sensor generano e ricevono dati e informazioni che vanno oltre i classici segnali di commutazione o i parametri di processo misurati. Pertanto, essi consentono un notevole incremento dell'efficienza, una maggiore flessibilità e una migliore pianificazione grazie alla manutenzione predittiva dell'impianto. Per rispondere alle diverse esigenze applicative, i sensori intelligenti devono soddisfare quattro caratteristiche tecnologiche: sensibilità avanzata (massima affidabilità nel rilevamento di oggetti e raccolta dei valori di misura); comunicazione efficiente (robusto canale di comunicazione per una gestione Plug-and-play); diagnostica (costante autocontrollo del sensore e un monitoraggio dei parametri di processo per una manutenzione predittiva dei dispositivi e dell'impianto); possibilità di compiere "smart task" (sia funzioni aggiuntive intelligenti all'interno del sensore, sia possibilità di comunicazione diretta tra diversi sensori per ottenere soluzioni più veloci, efficienti ed economicamente vantaggiose).

I sensori intelligenti di tipo industriale, rispetto a quelli "civili", sono più resistenti e adatti per un contesto di fabbrica e sono costruiti per sopportare temperature, pressioni e vibrazioni estreme. Questi sensori sono ampiamente impiegati sia nelle industrie di processo (aziende energetiche e petrolifere, gestione acque, alimentari, minerarie, cartiere) che in quelle manifatturiere (settore automobilistico, elettrico ed elettronico) anche se le prime hanno un'importanza maggiore in termini di quote di mercato.

Sensori intelligenti e IoT

I sensori intelligenti rappresentano un fattore chiave di successo nel campo IoT. Le applicazioni IoT, siano esse usate da infrastrutture cittadine, impianti di processo o dispositivi indossabili (wearable), impiegano grandi matrici di sensori che raccolgono e trasmettono dati via internet a risorse centrali di elaborazione allocate in cloud. I software di analytics eseguiti su queste risorse trasformano l'enorme mole dei dati generati in informazioni fruibili dagli utenti e dai sistemi attuatori.

Per svolgere le loro funzioni come componenti IoT, oggi i sensori hanno bisogno di aggiungere alle loro funzioni base le seguenti proprietà: devono essere *low-cost*, così da essere impiegati su larga scala; molto piccoli, in modo da scomparire discretamente nell'ambiente; *wireless*, dato che una connessione con filo non è quasi mai praticabile; devono avere funzionalità di auto-identificazione e validazione; consumare poco, in modo da sopravvivere anni senza bisogno di cambiare la batteria, o essere dotati di una buona gestione di raccolta energetica; devono essere resistenti, in modo tale da minimizzare o eliminare il bisogno di manutenzione; avere funzionalità di auto-diagnosi e riparazione, oltre che di auto-calibrarsi o di accettare comandi da un collegamento wireless; infine, devono essere in grado di pre-processare dati per ridurre il carico su portali, PLC e risorse cloud.

Una caratteristica più avanzata, inoltre, è la capacità di combinare e correlare informazioni da più sensori per dare informazioni su eventuali problemi interni. Ad esempio, i dati di un sensore di temperatura e quelli di un sensore di vibrazione possono essere usati per individuare la causa di un fallimento meccanico. In alcuni casi, le due funzioni sono disponibili in un solo dispositivo, in altri le funzioni sono combinate a livello software per creare un "soft" sensor.
Se ben calibrato, il sensore può lavorare "per eccezioni" trasmettendo dati solo se i valori della variabile misurata cambiano significativamente rispetto al campione. Questo riduce sia il carico sulla risorsa centrale di elaborazione, che la richiesta energetica dello smart sensor.
Quando il sensore intelligente comprende almeno due rilevatori nella sonda, le funzionalità di auto-diagnostica possono essere costruite internamente, individuando eventuali deviazioni di un elemento sensore rispetto all'altro. Oltretutto, nel caso uno dei due rilevatori si guasti, per esempio a causa di un corto-circuito, il processo può continuare con il secondo elemento di misura. La sonda può anche sfruttare l'attività dei due rilevatori in contemporanea per migliorare la risposta di monitoraggio.

Fabbricazione di un sensore intelligente

I metodi di produzione dei sensori intelligenti devono portare a ridurre sempre di più le loro dimensioni, il loro peso, il consumo di energia e il costo del sistema e dei suoi componenti. La stessa tendenza bisogna applicarla anche al packaging, che costituisce l'80% del costo generale e influisce sulla forma.

Fig. 2B – Sensore Tinynode B4

Fig. 2A – Sensore Tinynode A4

Gli smart sensor vengono creati integrando gli elementi di un sistema micro-elettromeccanico (MEMS) con circuiti integrati CMOS, che offrono tutte le funzioni di supporto, amplificazione ed elaborazione del segnale. In origine, la tecnologia Wafer Level Vacuum Packaging (WLVP) usata includeva solo sensori discreti, e i sensori intelligenti venivano realizzati collegando chip MEMS discreti ai circuiti integrati attraverso il package o un substrato a scheda con un approccio chiamato integrazione multi-chip. Un approccio migliorato permette di interconnettere il circuito integrato CMOS e gli elementi del sensore direttamente, senza l'uso di schede, con un sistema di tipo system-on-chip (SoC), più complesso del precedente ma con vantaggi di maggiore densità e minori costi.

Uno sguardo al mercato

Secondo un recente studio della Global Market Insights, il mercato dei sensori intelligenti nel 2015 superava i 20 miliardi di dollari, con un tasso annuo di crescita composto (CAGR, Compounded Average Growth Rate) di oltre il 17% dal 2016 al 2024.
L'intero mercato degli smart sensor è guidato dalle iniziative favorevoli dei governi, dai progressi nell'elettronica di consumo e nell'industria aerospaziale e della difesa, e dalla crescente tendenza alla miniaturizzazione. Le amministrazio-

ni governative in particolare stanno investendo a livello globale in modo crescente su larga scala in queste tecnologie, mentre i costruttori stanno progredendo nella miniaturizzazione attraverso opzioni di montaggio flessibile, dimensioni sempre minori e incorporando diverse funzionalità su un singolo chip.
Il mercato sarà trainato nei prossimi anni, in particolare, dalle applicazioni automobilistiche, aerospaziali e, in minor misura, dal settore dei robot industriali.
L'emergere di tendenze come le smart city, la domotica e la home security offrono ulteriori opportunità di crescita. In queste applicazioni i sensori intelligenti vengono usati per funzionalità di monitoraggio attivo di città, case e persone, in termini di sicurezza e sorveglianza e per minimizzare i costi della sanità attraverso dispositivi wearable di controllo continuo e assistenza del paziente.
Inoltre, gli smart sensor stanno assumendo un ruolo fondamentale anche nell'affrontare le sfide dell'ambiente, in quanto utilizzati nel monitoraggio e riduzione dei livelli di inquinamento.
Grazie soprattutto alla crescita dei dispositivi IoT e a una spinta della domanda nell'impiego di tecnologie indossabili (wearable), in particolare gli smart watch, si prevede una crescita delle tecnologie MEMS a un tasso annuo di crescita composto di oltre 15% dal 2016 al 2024.
Le Wsn (wireless sensor networks, reti di sensori wireless) saranno protagoniste di una significativa crescita grazie all'alta velocità e ai prezzi contenuti. La domanda di smart sensor si alzerà anche per effetto della crescente adozione di reti wireless negli spazi commerciali, volte a sostituire le reti cablate per l'incapacità di queste ultime di supportare un grande numero di dispositivi e per ragioni di efficienza e velocità di connessione.
Si prevede inoltre un incremento dell'utilizzo dei sensori smart in applicazioni nell'industria aerospaziale e della difesa in particolare per tecnologie di rilevazione e misura di gas (monossido di carbonio, ossigeno ecc.) in velivoli aerei e aerospaziali.

Un esempio di applicazione

Tinynode è un'azienda svizzera, parte di Paradox Engineering, specializzata in soluzioni Smart Parking e sistemi wireless per il rilevamento di veicoli (www.pdxeng.ch) che ha sviluppato dei sensori intelligenti dedicati a questo tipo di applicazioni.

Fig. 3 – Esempio di applicazione dei sensori intelligenti Tinynode

I dispositivi A4 e B4 (Fig. 2A e 2B) rilevano la presenza di un veicolo in uno stallo di sosta e, attraverso una rete wireless, trasmettono i dati a un sistema centrale, grazie al quale il gestore del parcheggio può monitorare in tempo reale l'occupazione dei singoli posti auto, la durata della sosta ed eventuali abusi (es. sosta oltre il tempo consentito, presenza di un mezzo pesante in uno stallo destinato alle auto ecc.).
Il sensore A4 è progettato per essere installato sopra la superficie stradale, mentre il B4 deve essere affondato nel manto d'asfalto (Fig. 3). Entrambi i dispositivi operano su frequenze sub-GHz (in particolare 868 MHz, 915 MHz o 920 MHz), garantiscono una disponibilità radio superiore al 99%, un'accuratezza nel rilevamento dei veicoli di oltre il 98% e una vita utile delle batterie fino a 10 anni.
Offrono un grado di protezione IP68 e, grazie alla recente revisione della posizione dei componenti interni e del layout PCB, assicurano maggiore resistenza alle sollecitazioni meccaniche, come ad esempio il lavaggio della strada o lo spazzamento della neve, alle vibrazioni, gli sbalzi di temperatura e l'umidità. Possono quindi essere installati in qualsiasi ambiente sia indoor sia outdoor, anche in condizioni meteo disagevoli.
Sono inoltre disponibili le versioni A4-H e B4-H per le soluzioni Smart Parking dedicate ai mezzi pesanti.
Il sistema è stato attivato già in alcune installazioni nelle città di Pola (Croazia) e di Kolin (Repubblica Ceca), e nel campus dell'Università della California a San Diego (USA).

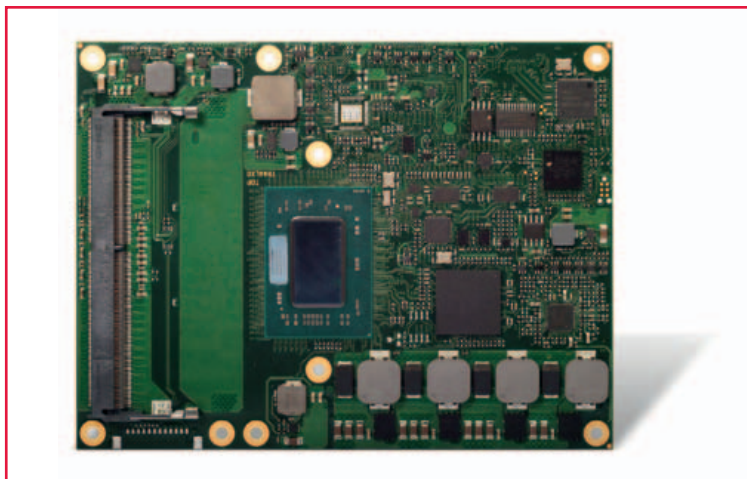
Moduli COM: un nuovo punto di riferimento per l'elaborazione embedded di fascia alta

La rivalità con l'architettura x86 si è di nuovo riaccesa. Con l'introduzione dei processori AMD Ryzen Embedded, AMD ha fissato un nuovo punto di riferimento grazie a una grafica eccellente e un incremento del 50% delle prestazioni di elaborazione. Elementi più che sufficienti per indurre congatec a utilizzare questi nuovi processori per i propri moduli in formato COM Express con pinout Type 6

Martin Danzer
Director Product Management
congatec

I moduli COM Express con pinout Type 6 sono la soluzione standard per le applicazioni di elaborazione embedded di fascia alta. Questi moduli, caratterizzati da ingombri (footprint) e interfacce standardizzate, sono utilizzati dagli sviluppatori per il progetto dei loro sistemi custom. Essi hanno a disposizione una sorta di super-componente ad alto grado di integrazione corredato da un BSP (Board Support Package) "application ready" e supportato da numerose guide alla progettazione e schemi circuitali utili per lo sviluppo di schede carrier specifiche. Rispetto a una progettazione full-custom, i moduli COM permettono di ridurre i costi di NRE in misura compresa tra il 50 e il 90%. La compatibilità con lo standard COM Express definito da PICMG permette di utilizzare Computer-on-Module conformi a questo standard realizzati da vari costruttori con differenti configurazioni di processore. Ciò contribuisce ad aumentare la durata dei progetti dei sistemi, oltre a garantire un'elevata scalabilità.

Applicazioni embedded a elevate prestazioni

La scalabilità è un aspetto particolarmente significativo per tutte quelle applicazioni che richiedono le più avanzate prestazioni grafiche e di elaborazione. Nel settore embedded, in particolare, si possono annoverare le seguenti:

A) Il modulo conga-TR4 con processore Ryzem embedded di AMD: un punto di riferimento per il moduli in formato COM Express con pinout Type 6

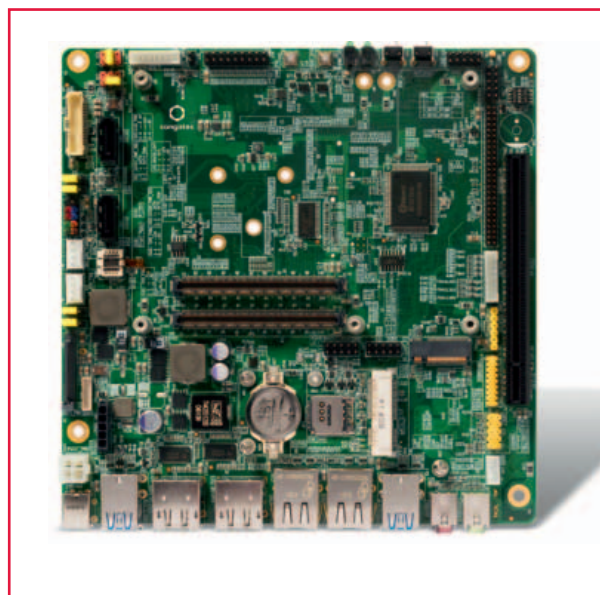
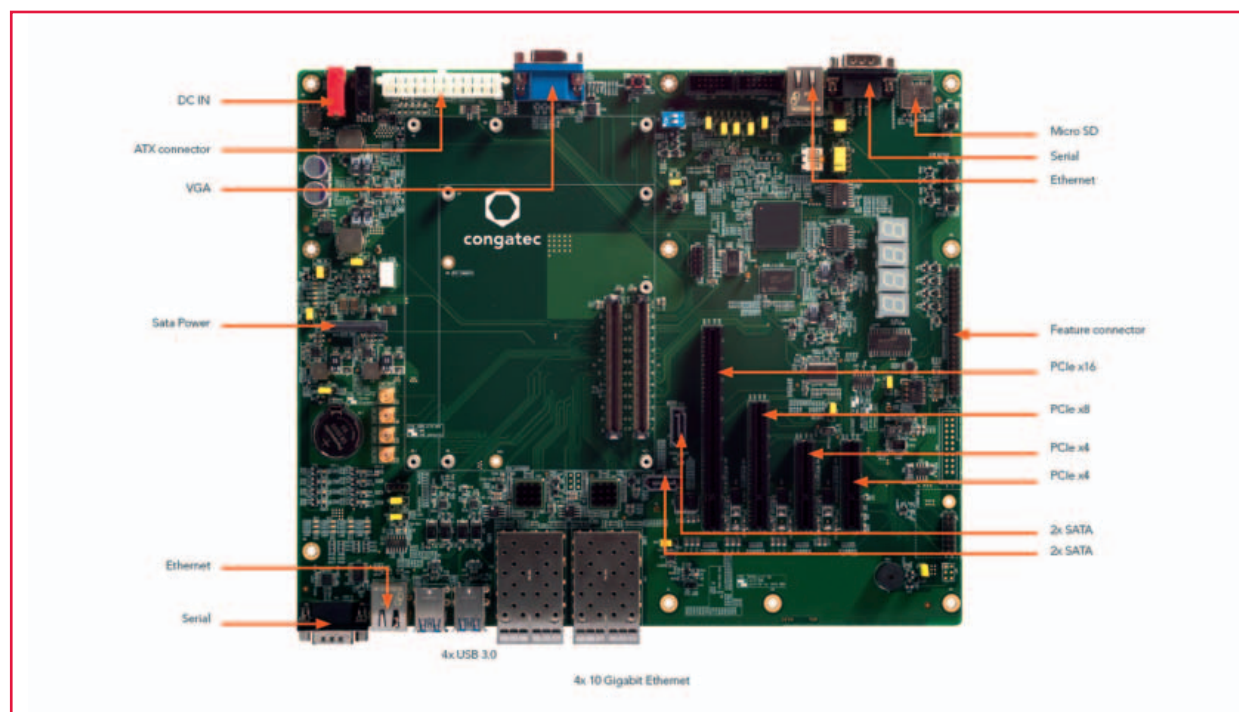
- Imaging in campo medicale, perché ad una maggiore precisione dei sistemi di visualizzazione corrisponde la possibilità di effettuare diagnosi migliori e più efficaci.
- Macchine da gioco, in quanto devono essere in grado di attrarre i giocatori con animazioni 3D di elevata qualità riprodotte su più schermi di dimensioni e con livelli di risoluzione via via maggiori.
- Suite per l'editing multimediale, che devono essere in grado di elaborare in tempi brevi contenuti con risoluzione di 4k o superiori.
- Sistemi di cartellonistica digitale (digital signage) e simulatori, per i quali valgono le medesime considerazioni, oltre a workstation presenti nelle sale controllo e sistemi per il controllo della qualità di tipo ottico.
- Robotica "intelligente" e veicoli a guida autonoma che utilizzano algoritmi di "deep learning" per ottimizzare la consapevolezza del contesto in cui operano (situational awareness).

Moduli per garantire maggiori prestazioni in tempi brevi

Nel momento in cui i progettisti di sistemi come quelli appena menzionati o di altri apparati ad alte prestazioni possono sfruttare le potenzialità dei processori delle più recenti generazioni mediante la semplice sostituzione di un modulo è chiaro che è possibile introdurre sul mercato soluzioni in grado di offrire prestazioni decisamente superiori in tempi brevi. Grazie al significativo aumento di prestazioni che sono in grado di garantire, i processori Ryzen V Series di AMD fissano un nuovo punto di riferimento nel settore dell'elaborazione embedded di fascia alta.

Prestazioni grafiche senza rivali

A differenza dei concorrenti diretti, AMD può contare su una divisione specializzata nello sviluppo di schede grafiche che realizza anche le unità grafiche dei processori embedded. Ciò consente ai processori di nuova generazione di sfruttare tutti i vantaggi della tecnologia grafica più avanzata disponibile. La GPU integrata nei nuovi processori, basata sulla più recente architettura Radeon Vega di AMD, garantisce prestazioni grafiche più che doppie rispetto a quelle del suo predecessore. I benchmark effettuati su dispositivi con un livello di dissipazione di 15 W evidenziano un incremento delle prestazioni fino al 228%. Alla base si questo sensibile aumento delle prestazioni vi è l'architettura Graphics Core Next, caratterizzata da velocità di clock più elevate e dall'apporto di numerose altre migliorie.

Per gli sviluppatori, i vantaggi legati a questo aumento delle prestazioni non si limitano solamente

B) La scheda madre conga-IT6 in formato Mini-ITX di congatec può essere equipaggiata con il nuovo modulo per poter essere integrate in ogni alloggiamento di sistema in formato ATX

C) Scheda carrier di valutazione per pinout Type 6. Tutte le funzioni del nuovo modulo in formato COM Express con pinout Type 6 possono essere verificate in modo esaustivo con la scheda carrier conga-X7/EVAL

alla maggiore velocità di calcolo della frequenza dell'immagine nelle animazioni 3D, ma coinvolgono anche le funzionalità di presentazione. Per esempio ora è possibile erogare singoli contenuti a quattro (invece che a tre) display con risoluzione 4k (Ultra HD). Nel caso di immagini particolarmente realistiche con elevato contrasto e un ampio spazio colore (wide colour gamut), la nuova grafica Vega supporta ora display HDR (High Dynamic Range) - una tecnica che permette di migliorare la qualità dei singoli pixel - con una profondità di 10 bit per canale colore. Tale caratteristica risulterà molto utile per i sistemi diagnostici avanzati usati in campo medicale oltre che per le applicazioni di cartellonistica digitale particolarmente coinvolgenti (immersive) e videogiochi. Per assicurare che i segnali grafici siano visualizzati con la massima ampiezza di banda possibile, la grafica Vega prevede il supporto delle più recenti tecnologie di interfaccia - fino a quattro DisplayPort 1.43, HDMI 2.0b ed eDP 1.4. Oltre a ciò, l'elaborazione dei file video è accelerata via hardware, senza quindi coinvolgere la CPU: è prevista la possibilità di decodificare video compressi nei formati H.265 a 10 bit e VP9. Grazie all'engine di compressione video H.264 (profilo 3.1) è anche possibile codificare due flussi video in risoluzione full-HD a 8 bit in tempo reale.

Incremento fino al 52% delle prestazioni di elaborazione

I nuovi processori multicore assicurano notevoli incrementi delle prestazioni complessive per le applicazioni single-thread e multi-thread. Il nuovo core Zen, ad esempio, è in grado di gestire un numero di istruzioni per ciclo superiore del 52% rispetto al suo predecessore, il core Excavator. Questo significativo incremento di prestazioni è ascrivibile alle numerose migliorie apportate alla nuova microarchitettura Zen. Per esempio i nuovi processori Ryzen embedded supportano per la prima volta il multi-threading simultaneo (STT - Simultaneous Multi-Threading). Grazie ad esso è ora possibile elaborare due thread in parallelo, con conseguente aumento del throughput. Un'altra caratteristica che contribuisce a incrementare le prestazioni è Precision Boot, che ottimizza su base individuale la frequenza di clock per ciascun core. La funzionalità Extended Frequency Range, inoltre, permette di aumentare la frequenza di clock al di sopra di quella prevista dalle specifiche in funzione del margine termico disponibile.

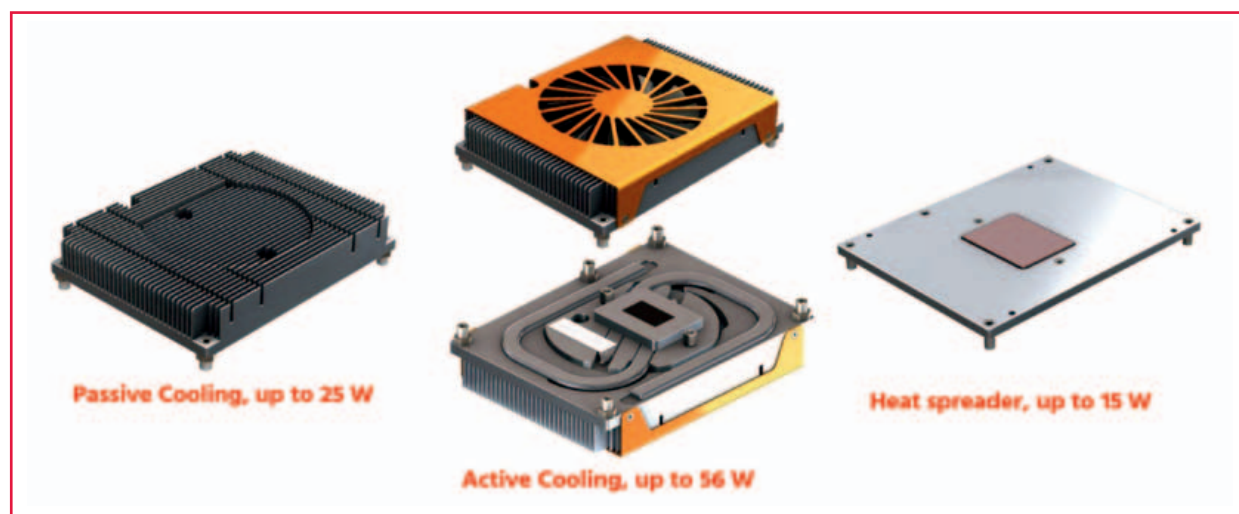
Intelligenza artificiale per aumentare l'efficienza complessiva

I core Zen sono dotati di un'intelligenza artificiale grazie alla presenza di una rete neurale (Neural Net Prediction) che, come dice il nome stesso, consente al processore di prevedere il percorso di elaborazione che verrà intrapreso da un'applicazione sulla base dei flussi del programma precedenti. La funzionalità Smart Prefetch, inoltre, fa ricorso a sofisticati algoritmi di apprendimento per tracciare il comportamento del software al fine di anticipare le richieste di un'applicazione e preparare i dati necessari in anticipo, contribuendo in tal modo a incrementare l'efficienza complessiva del sistema.

Miglior rapporto tra prestazioni e consumi

Tutte le migliorie e gli incrementi in termini di prestazioni finora descritti sono ottenuti a fronte di un TDP (in pratica la dissipazione termica) ottimizzato, elemento essenziale per consentire l'integrazione dei nuovi processori in sistemi embedded dove lo spazio è sempre un fattore critico. L'ottimizzazione del TDP è dovuta, fra l'altro, all'uso dei transistor FinFET per i core Zen, realizzati in tecnologia da 14 Nm, che permettono anche di ridurre le dimensioni del chip grazie alla maggiore densità di packaging. L'ottimizzazione del TDP assume una particolare rilevanza in numerose applicazioni embedded. Si può tranquillamente affermare che il livello di prestazioni che in passato era possibile ottenere con un TDP di 45 W, sono ora conseguibili con un TDP di circa 30 W. Nel caso di sistemi privi di ventole e con raffreddamento di tipo passivo, l'incremento di prestazioni è di assoluto rilievo. I test condotti hanno evidenziato che con un cTDP compreso tra 15 e 25 W, il processore Ryzen V1605B di AMD - che è confrontabile con il processore mobile Ryzen 5 2500U - ha ottenuto un punteggio di 10,377[1] nella prova effettuata con il programma Geekbench (di tipo multi-threaded), mentre una CPU Intel Core i7 7600U equivalente si è fermata a 8,401 punti. La CPU i7-8550U Gen8, con un punteggio di 11,418, garantisce un miglioramento pari a circa il 10% in termini di prestazioni ma il suo prezzo attuale, pari a 409 dollari, è significativamente più elevato[2].

Quelle appena descritte sono caratteristiche di tutto rilievo, in termini sia di elaborazione sia di grafica, disponibili a un costo senza dubbio competitivo. Gli sviluppatori che desiderano valutare in tempi brevi e utilizzare i nuovi processori Ryzen embedded V-Series possono ora integrare nelle loro schede carrier i nuovi moduli COM di congatec o collaudarne le potenzialità con la scheda carrier di valutazione per moduli in formato COM Express con pinout Type 6. Per ciascuna categoria di valori di TDP sono disponibili le appropriate soluzioni di raffreddamento, in modo da poterle integrare in modo estremamente semplice.

Moduli COM per sfruttare in tempi brevi le potenzialità dei nuovi processori congatec ha già collaudato con risultati molto positivi il nuovo modulo conga-TR4 in numerosi progetti di siste-

D) La standardizzazione del formato COM Express relativamente al sistema di raffreddamento è completa ed esaustiva per cui non è richiesta nessun onere di progettazione per equipaggiare i sistemi con nuovi moduli caratterizzati da un TDP compatibile

mi. Gli sviluppatori di un'azienda partner, ad esempio, per eseguire la migrazione del modulo su un sistema esistente dovevano impiegare lo stesso tempo di quello richiesto per equipaggiare il sistema con un hardware che era già stato valutato. Per le routine di installazione necessarie per l'impostazione del software, inoltre, era richiesto l'utilizzo delle normali procedure. Grazie alle API standardizzate, identiche per tutti i moduli congatec, non è stato richiesto nessun onere di programmazione aggiuntivo per soddisfare le esigenze l'hardware. Ciò implica, tra l'altro, che il controllo del GPIO richiesto dai progettisti per eseguire le misure di temperatura del sistema al fine di controllare la luminosità del display, è identico per ciascun modulo.
Questo esempio di migrazione evidenzia il fatto che nel caso di un progetto basato sui moduli COM, l'utilizzo dei processori delle più recenti generazioni è un processo semplice che non comporta problemi di sorta. Per la migrazione da una generazione di processori all'altra, in sostanza, è sufficiente tenere in considerazione il TDP. Questo approccio è utile anche per le motherboard (schede madri) standard, come quelle utilizzate nelle applicazioni medicali di fascia alta, perché gli unici costi sostenuti per la certificazione dei nuovi moduli sono quelli necessari per certificare i moduli stessi. Grazie all'elevata standardizzazione, sono disponibili schede carrier per questo scopo, insieme a un'ampia documentazione. congatec, per esempio, pone grande enfasi sull'assicurare che ogni modulo sia corredato con un'esaustiva documentazione tecnica, particolarmente utile per la certificazione dei singoli moduli.

I moduli COM semplificano la migrazione

Grazie alle API standardizzate e al supporto BSP, è stato possibile effettuare la migrazione di un sistema caratterizzato da un TDP di 25 W – in precedenza equipaggiato con altri tipi di processore – su un modulo COM basato sui nuovi processori Ryzen embedded V-series nel giro di un'ora. Poiché COM Express prevede la standardizzazione sia a livello di footprint sia a livello di progetto del dissipatore, non sono stati richiesti oneri di design aggiuntivi. La migrazione di sistemi in cui il processore è direttamente integrato sulla scheda attraverso uno zoccolo o un package BGA è un'operazione senza dubbio più complessa.

Moduli COM: la soluzione ideale per schede Mini-ITX

Per questa ragione, congatec ha recentemente introdotto una scheda madre (motherboard) in formato Mini-ITX. Essa abbina le interfacce standard delle applicazioni embedded con funzionalità tipiche del mondo IT per soddisfare le esigenze delle workstation grafiche ad alte prestazioni e dei mini-server. Per il collegamento di schede grafiche a elevate prestazioni e GPGPU è disponibile uno slot PCIe con un massimo di 16 canali (lane) in funzione del modulo. Tra le altre periferiche disponibili da segnalare 4 porte USB e una porta miniPCIe. I monitor possono essere collegati mediante 2 interfacce DP, 2 HDMI o mediante porte eDP, LVDS e VGA. Grazie a 2 porte 1 GbE con controllore di rete dedicato Intel i211 e uno slot micro-SIM è garantita la massima flessibilità in termini di connettività. Per quel che riguarda i supporti di memorizzazione sono invece disponibili 2 porte SATA Gen3 oltre a uno slot per schede microSD e un socket M.2 type B che supporta la memoria Intel Optane ad alta velocità. In termini di interfacce embedded questa nuova scheda madre è equipaggiata con 4 porte COM (232/422/485), 1 porta GPIO (4x GPIs, 4x GPOs and 16x GPIOs) e 1 per bus I²C. Il supporto di un'ampia gamma di tensioni di ingresso interne ed esterne (da 12 a 24 VDC) assicura la massima flessibilità in termini di alimentazione e, grazie al modulo Smart Battery Management è possibile implementare anche applicazioni mobili alimentate a batteria. Una vasta scelta di accessori - che comprende pannelli di I/O, kit di cavi e adattatori video - permette di semplificare la fase di integrazione.

Bibliografia

[1] *https://hothardware.com/reviews/amd-ryzen-5-2500u-benchmarks-revisited-hp-envy-x360-ssd-update*
[2] *Retrieved on 21 January 2018 from https://ark.intel.com/products/122589/Intel-Core-i7-8550U-Processor-8M-Cache-up-to-4_00-GHz*

VME: uno standard datato ma ancora vigoroso

Sia dai dati di mercato, sia dalle iniziative di sviluppo di nuove board e sistemi, VMEbus (VersaModular Eurocard bus) risulta essere ancora una tecnologia viva e vegeta, in grado di evolversi e aprirsi ad applicazioni che sanno estendersi oltre quelle tradizionali

Giorgio Fusari

Il segmento di schede embedded basate su tecnologia VME, o VMEbus, sta contribuendo in maniera significativa al rafforzamento della quota di mercato posseduta dai computer su scheda singola, o "single board computer" (SBC). Ma esso stesso è ancora in espansione e, in particolare, VME è previsto crescere con un CAGR (tasso di crescita annuale composto) di oltre il 10% dal 2016 al 2024. La stima proviene da una recente ricerca della società di analisi di mercato Global Market Insights, ed è motivata da due ragioni fondamentali. In primo luogo ci sono le caratteristiche di alta affidabilità della tecnologia VME in applicazioni industriali di tipo "rugged", come il controllo di motori e attuatori, o in progetti per il settore militare e della difesa. In secondo luogo, VME è concepita come una piattaforma con una funzionalità integrata per il completo supporto del multi-processing. Questa capacità di supportare l'uso di molteplici CPU, unitamente alla disponibilità di opzioni di elaborazione realtime, permette di incrementare le prestazioni e la banda di elaborazione in diversi tipi di applicazioni.
Un'altra categoria di prodotti con una presenza significativa nel mercato dei SBC è quella delle schede basate su tecnologia CompactPCI (cPCI), che ha mantenuto una quota di fatturato di oltre il 25% nel 2015. Tra le caratteristiche chiave delle schede cPCI, la società di analisi indica soprattutto la robustezza, la modularità, la possibilità di ottenere soluzioni standardizzate per ambienti severi (rugged). Inoltre, quando queste piattaforme vengono integrate con i SBC riescono a fornire soluzioni convenienti, in termini di costo e longevità del progetto.
Schede VME, cPCI e altre categorie di board, grazie alle molte e importanti applicazioni embedded collegate, stanno facendo espandere il mercato dei SBC a forte ritmo, con un CAGR del 12,5% che dovrebbe portarlo a raggiungere 1,2 miliardi di dollari per il 2024. Più in dettaglio, la crescita del comparto dei computer SBC appare indirizzata dalla crescente penetrazione nel settore della sanità: i SBC risultano infatti integrati su larga scala nelle attrezzature medicali, per il fatto di possedere alta

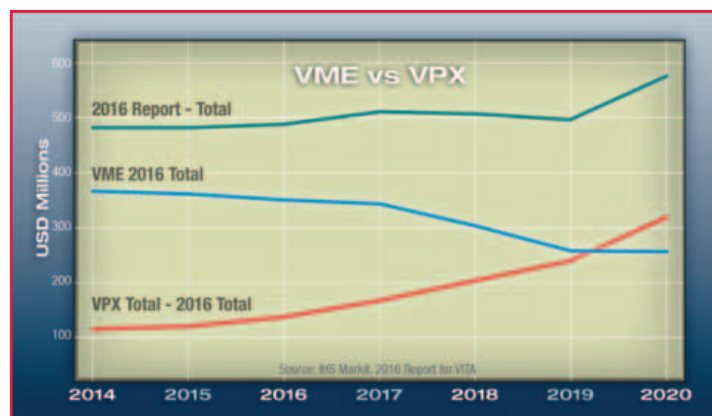



Fig. 1 – Le vendite di schede e sistemi embedded VME verranno superate da quelle di prodotti VPX solo nel 2019
(Fonte: IHS Markit, 2016 Report for VITA)

affidabilità e capacità di fornire soluzioni e servizi efficienti nel mondo "healthcare". Per di più, viene segnalata la crescente utilizzazione di questi computer in altre applicazioni medicali, come i sistemi medicali di monitoraggio personalizzati, i dispositivi elettronici medicali e i computer indossabili "fault tolerant". Per il futuro, la crescente domanda nel comparto delle applicazioni Internet of Things (IoT) è prevista stimolare ulteriormente lo sviluppo del mercato dei SBC.

Fig. 2 – La scheda VME Curtiss-Wright VME-690 (Fonte: Curtiss-Wright)

VME resiste al tempo

Anche in un contesto tecnologico in rapida evoluzione come quello attuale, non sempre succede che il mercato decreti con facilità la sostituzione di una tecnologia, soltanto perché questa risulta parecchio datata, e va necessariamente rimpiazzata con qualcosa di più moderno. Un principio, quello di prolungare la longevità dei sistemi, valido in particolar modo nel mondo embedded, e applicabile al caso della tecnologia VME. Sviluppato in origine nel 1981, lo standard VME definisce varie specifiche costruttive della scheda, tra cui quelle meccaniche, che comprendono le dimensioni della board, le specifiche dei connettori, le caratteristiche della enclosure; ma anche le specifiche elettriche del sistema, le tecniche di trasferimento dati. La successiva introduzione della specifica VME64, che supporta una velocità di 80 MB/s, stabilisce un framework per architetture di computer a 8, 16, 32 e 64 bit che

Fig. 3 – La scheda cPCI Serial Space di MEN Mikro Elektronik (Fonte: MEN Mikro Elektronik)

possono implementare sistemi a singolo processore o sistemi multiprocessore. VME è adottato in molteplici applicazioni, tra cui quelle più popolari sono i controlli industriali nell'automazione di fabbrica, e nella robotica; gli utilizzi nel settore militare, ad esempio nei sistemi di controllo di radar di terra e di velivoli; ma ci sono anche le applicazioni aerospaziali, nei sistemi di controllo delle reti di trasporto (ferrovie), nelle telecomunicazioni, nei dispositivi medicali.
Per anni, e a varie riprese, nel mercato si è avuta la sensazione che VME potesse essere abbandonato, e sostituito da schede e computer con architetture più moderne. E se questo può essere in parte vero per alcuni settori, lo è di meno per ambiti come quello militare, in cui un requisito chiave è avere lunghi cicli di vita per i prodotti: qui il progetto si valuta con molta attenzione, prima di soppiantare una implementazione VME, compromettendo tutti i relativi investimenti, ivi compreso il tempo e il denaro impiegati per sviluppare e certificare il sistema. Senza poi considerare che, in tal caso, sono comunque necessarie, e vanno messe in conto, altre risorse per sviluppare e certificare un sistema completamente nuovo. In questi casi, quindi, se una data applicazione non ha l'esigenza di possedere tutte le nuove funzionalità di un'architettura più moderna, si tende a mantenerla e, semmai, ad aggiornarla. Non per nulla, il mercato totale delle schede VME risulta al momento ancora più grande di quello delle schede e sistemi VPX, come emerge dai dati di un rapporto della società di analisi IHS Markit, secondo cui le vendite di prodotti VPX incroceranno, superandole, quelle di sistemi VME solo nel 2019. Sempre secondo la società, il comparto VME, assieme a quello VPX, costituisce una quota notevole del mercato globale delle schede e computer embedded: la stima del fatturato VME-VPX risulta in crescita, dai 493 milioni di dollari del 2015, ai 576 milioni nel 2020, con un CAGR del 3,2%. E ciò in virtù della tendenza a espandere il dominio di queste board, dai consolidati spazi di mercato nel settore militare e aerospaziale, a settori come quello ferroviario, dove, per treni e altri veicoli commerciali, esistono analoghi requisiti tecnici in termini di resistenza e robustezza di funzionamento in ambienti severi, oltre che di durevolezza ed estensione del ciclo di vita dei prodotti.

Meglio aggiornare che sostituire

Di esempi di come le schede VME stiano evolvendosi per modernizzare i sistemi ve ne sono molti: all'inizio del 2017 Abaco Systems ha introdotto due SBC (XVB603 e XVR19) VME 6U, basati sulla settima generazione di tecnologia Intel (nome in codice "Kaby Lake"), e concepiti per coprire tutta la gamma di applicazioni di elaborazione di VME: dal controllo industriale, alle implementazioni totalmente "rugged", in utilizzi "mission critical" come quelli nel settore aerospazio e difesa. Molto più recente è il prodotto rappresentato da VME-690, un modulo switch Gigabit Ethernet (GbE) VMEbus 6U a 24 porte, introdotto a dicembre 2017 dalla divisione Defence Solutions di Curtiss-Wright.
Con il supporto integrato di fino a 24 interfacce GbE, VME-690 si posiziona sul mercato come la terza generazione di switch GbE VME della società, e punta a fornire una soluzione a basso consumo di energia (circa 35 W), e compatibile a livello di pin, per aggiornare i precedenti progetti VME, ai quali permette di aggiungere funzionalità evolute di sicurezza dei dati.
Il dispositivo VME-690, dichiara Curtiss-Wright, abilita i progettisti di sistema a modernizzare i propri sistemi VME legacy, e assicura che i nuovi progetti abbiano accesso alla più recente tecnologia di securizzazione delle comunicazioni dati. Attraverso VME-690, i system integrator hanno la possibilità di portare nuove funzionalità nelle piattaforme esi-

stenti, con espansioni che permettono di ottenere prestazioni migliorate e connessioni ad alta velocità nelle applicazioni con sensori avanzati. Con l'introduzione di VME-690, ha dichiarato Lynn Bamford, senior vice president e general manager di Curtiss-Wright Defense Solutions division, la società promuove il suo impegno a estendere la vita utile dei sistemi VME già realizzati. VME-690, sottolinea, è uno switch a 24 porte di categoria "rugged" che abilita gli utenti a costruire soluzioni "low-power" ad alte prestazioni, e al contempo indirizza le attuali e cruciali esigenze di cybersecurity.

cPCI Serial Space: porta CompactPCI nello spazio

Come sottolinea anche il consorzio PICMG, il successo dello standard CompactPCI è dovuto all'adozione del bus parallelo PCI (peripheral component interconnect) come bus dati principale, che lo ha reso uno dei primi bus universali adottati dai principali costruttori di microprocessori. Nelle applicazioni embedded, cPCI si presta all'utilizzo in molti settori: industria, aerospazio, settore militare, acquisizione dati, comunicazioni e quant'altro, anche se, in prospettiva, il trend di mercato a livello mondiale, sempre secondo IHS Markit, risulta in contrazione, registrando un CAGR pari a -7,9%, e un giro d'affari che scende, dai 202 milioni di dollari del 2015, ai 134 milioni di dollari del 2020. Se questi sono gli indicatori del mercato, le attività di sviluppo dello standard non si fermano: proprio nell'agosto 2017 il PICMG ha infatti ratificato la specifica cPCI Serial Space (CPCI-S.1 R1.0), che rappresenta una versione "ruggedized", irrobustita, di CompacPCI Serial, e indirizza in maniera specifica i requisiti di ambienti estremi come lo spazio. L'obiettivo è utilizzare il nuovo standard a bordo di satelliti per varie applicazioni, ma anche sulla Terra, integrandolo in sistemi di controllo e stazioni terrestri. In aggiunta, i convenzionali prodotti CompactPCI Serial possono essere combinati con i nuovi cPCI Serial Space per sviluppare sistemi di test e simulazione. CompactPCI Serial Space, sottolinea PICMG, è stato selezionato per il programma OneWeb, in cui 900 satelliti utilizzeranno la tecnologia.

Moduli COM: cresce il mercato, e il supporto di Qseven

Un settore delle schede embedded che non smette di crescere è quello del moduli COM (computer on module), per il quale IHS Markit calcola un CAGR pari a 8,6%, che incrementa il giro d'affari mondiale di questi prodotti dai 765,1 milioni di dollari del 2015, ai 1.157,2 milioni di dollari del 2020.

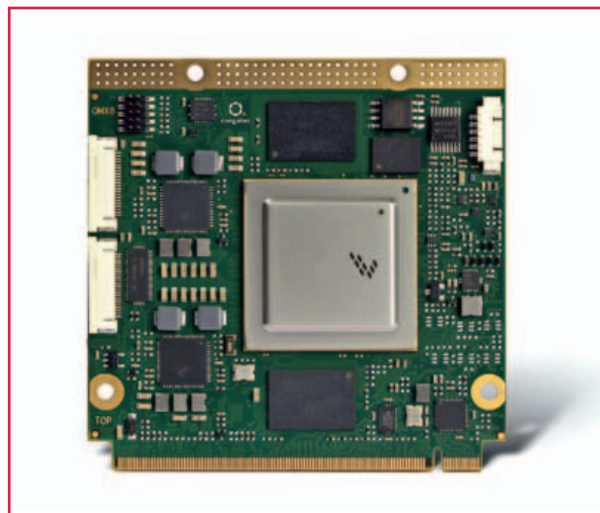



Fig. 4 – La scheda congatec conga-QMX8, nel form factor Qseven (Fonte: congatec)

Kontron, rafforzata dal recente completamento della fusione con S&T, è pronta a presentare a Embedded World 2018 di Norimberga nuovi moduli COM, per la prima volta dotati di formato Q7 (Qseven), in aggiunta a quelli di tipo COM Express e SMARC 2.0. Con i nuovi prodotti forniti nel form factor Q7, Kontron intende indirizzare i clienti che utilizzano già prodotti con questo formato, aprendo così un percorso di migrazione verso lo standard SMARC 2.0.

Ancora a proposito di Qseven, congatec ha di recente annunciato il supporto dei processori a 64 bit NXP i.MX8 per i moduli standard Qseven e SMARC. Come membro dell'EAP (Early Access Program) di NXP, congatec potrà introdurre questi moduli in contemporanea con l'introduzione della nuova famiglia di processori di NXP basati su core Cortex A53/A72 di ARM, consentendo agli utenti OEM di accelerare i progetti delle schede carrier per le proprie applicazioni. I nuovi moduli con form factor Qseven e SMARC sono in grado di operare nell'intervallo di temperatura esteso, compreso tra -40 e +85 °C, e l'obiettivo è farli penetrare in svariate applicazioni embedded: in campo industriale; a bordo di veicoli commerciali, come treni e bus, ma anche in veicoli elettrici e autonomi di nuova generazione.

Uno sguardo al mondo tecnologico di Arduino

Arduino è una scheda di sviluppo basata sul microcontrollore ATmega e disponibile in diversi fattori di forma e caratteristiche. Nata inizialmente per scopi hobbistici, Arduino si è presto dimostrata essere all'altezza per molte applicazioni in diversi campi industriali e commerciali, rappresentando, di fatto, una scheda base per una prima prototipazione rapida

Alberto Di Paolo

La scheda di sviluppo Arduino consta essenzialmente del microcontrollore ATmega attraverso il quale vengono gestiti i pin I/O per l'implementazione di schede esterne al fine di ottenere una facile implementazione e integrazione delle relative funzionalità. La piattaforma integra un regolatore di tensione e un'interfaccia USB sia per l'alimentazione sia per la programmazione. Un'interfaccia IDE facilita lo sviluppo del codice attraverso l'uso di algoritmi e funzioni in linguaggio C/C++. La scheda si presenta come un modello di prototipazione rapida per implementare diverse soluzioni in vari settori dell'IoT, grazie alla sua capacità di leggere sensori ambientali e condividere i relativi dati attraverso piattaforme cloud per la successiva gestione e analisi. In commercio ci sono molte schede Arduino, che si differenziano in termini di memoria, fattore di forma (per adattarsi al design del prodotto), clock e capacità di elaborazione del microcontrollore integrato.

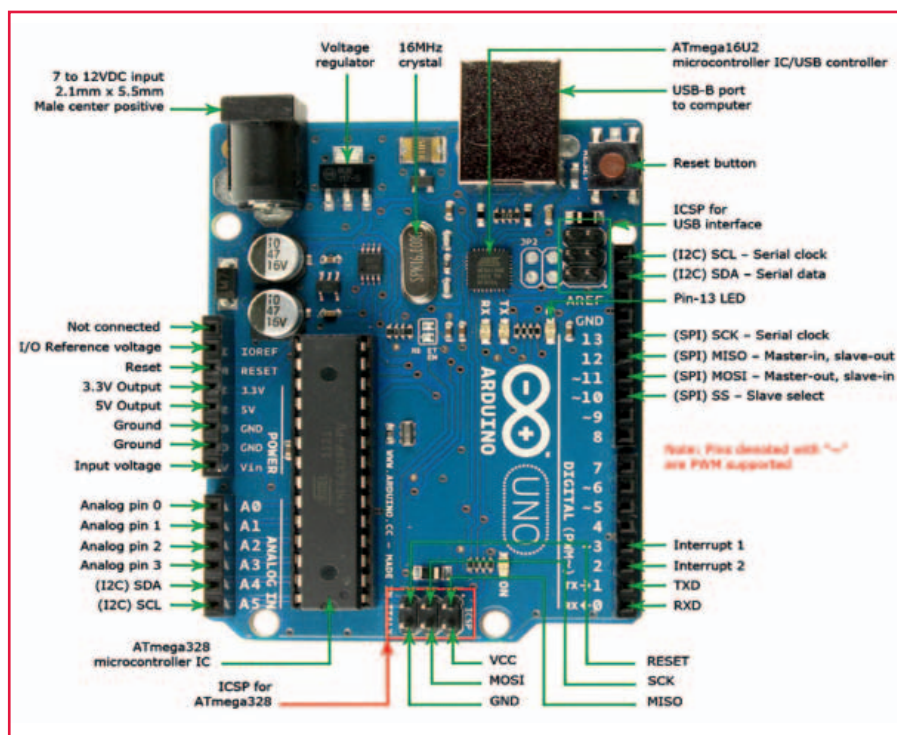



Fig. 1 – La piedinatura di Arduino UNO. I pin 2 e 3 sono relativi all'interrupt. L'oscillatore al quarzo è posizionato vicino al connettore USB

La tecnologia di Arduino

Un esempio tipico della famiglia Arduino è Arduino UNO, equipaggiata con un microcontrollore ATmega328 ospitato in package a 28 pin. La configurazione dei pin di Arduino UNO è mostrata nella figura 1.

La scheda Arduino UNO può essere alimentata da laptop tramite una sorgente USB o esterna come una batteria o un adattatore. Questa sche-

da può funzionare con un'alimentazione esterna con valori compresi tra 7 e 12 V e fornisce il riferimento di tensione attraverso il pin IOREF oppure mediante Vin. Sono previsti 14 pin di I/O digitali, ciascun dei quali assorbe e fornisce una corrente di 40 mA. Alcuni dei pin hanno funzioni speciali come 0 e 1 che fungono rispettivamente da trasmettitore e ricevitore. Tra i pin digitali, 3, 5, 6, 9 e 11 forniscono la PWM, mentre il pin 13 viene utilizzato per controllare il mini LED presente sulla scheda. Fondamentalmente, il processore della scheda Arduino utilizza l'architettura Harvard che prevede memorie separate per i dati e il codice programma. I dati vengono memorizzati nella memoria dati e il codice viene memorizzato nella memoria del programma flash. Il microcontrollore ATmega328 ha 32 kb di memoria flash, 2 kb di SRAM, 1 kb di EPROM e funziona con una velocità di clock di 16 MHz (Fig. 2).

Bitlash Software: Serial Command Input / Edit | Background Macro Tasker | Macros in EEPROM | Bitlash C API | Command Interpreter | Expression Parse / Eval | Built-in Functions | Print Formatter | Error Handling | Variable Storage | User Functions

Arduino Software: Arduino Runtime & Libraries | User Libraries | avr-gcc Runtime & Libraries

Arduino Hardware: Atmel ATMega328p MCU | EEPROM | Serial IO | Digital IO | Analog IO | Timers | Interrupts | RAM | Flash IO | et cetera

Fig. 2 – L'architettura di Arduino

Il principale vantaggio della tecnologia Arduino è quello di poter caricare direttamente i programmi nel dispositivo senza bisogno di un programmatore hardware. Ciò è possibile grazie alla presenza del bootloader che consente allo sketch di

```
Blink | Arduino 1.6.13
File  Edit  Sketch  Tools  Help
Blink
// the setup function runs once when you press reset or power the board
void setup() {
  // initialize digital pin LED_BUILTIN as an output.
  pinMode(LED_BUILTIN, OUTPUT);
}

// the loop function runs over and over again forever
void loop() {
  digitalWrite(LED_BUILTIN, HIGH);   // turn the LED on (HIGH is the voltage level
  delay(1000);                       // wait for a second
  digitalWrite(LED_BUILTIN, LOW);    // turn the LED off by making the voltage LOW
  delay(1000);                       // wait for a second
}
```

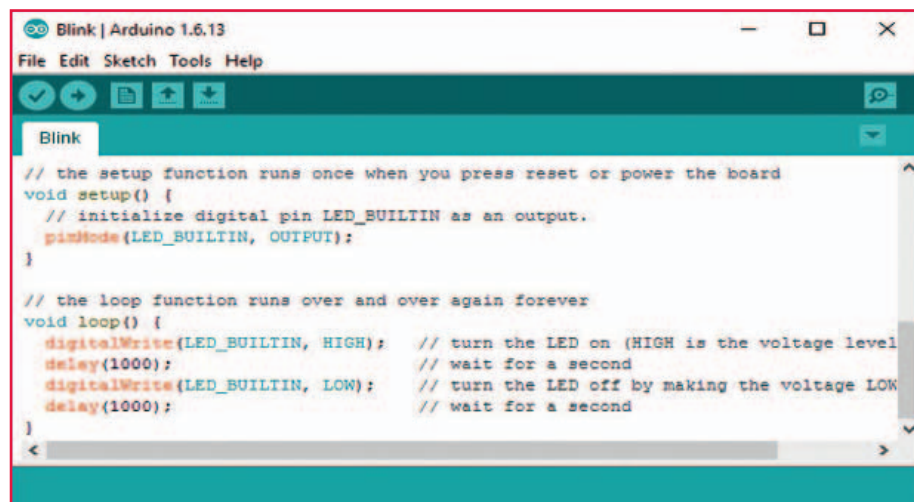



Fig. 3 – L'interfaccia IDE Arduino

essere caricato nell'hardware. La finestra IDE per la programmazione dello strumento Arduino contiene un editor di testo (impiegato per scrivere il codice), uno spazio messaggi (visualizza il feedback di compilazione), la console di testo e una serie di menu proprio come file, strumenti menu e modifica (Fig. 3).

I principali vantaggi della scheda Arduino sono il costo relativamente basso e la semplicità di configurazione e utilizzo (rispetto ad altre schede di sviluppo). Alcune delle caratteristiche chiave di Arduino UNO che si riflettono anche sulle altre tipologie presenti in commercio, possono essere riassunte nei seguenti punti:

- Design open source. Il vantaggio di essere open source è la grande comunità di persone che lo utilizzano, attraverso il quale è possibile risolvere molti problemi.
- Interfaccia USB. Il chip sulla scheda lavora direttamente con la porta USB e si registra sul computer come porta seriale virtuale. Ciò consente di interfacciarsi come un dispositivo seriale. Il vantaggio di questa configurazione è l'utilizzo della comunicazione seriale, unito alla semplicità dell'USB per il collegamento agli attuali computer moderni.
- Ottima gestione energetica e regolazione della tensione integrata. È possibile collegare una sorgente di alimentazione esterna fino a 12 V e regolarla sia a 5 V che a 3.3 V. Inoltre può essere alimentata direttamente da una porta USB senza alcuna alimentazione esterna.
- "Cervello" economico e di facile reperibilità. Il chip ATmega328, del costo di circa 3 euro, prevede innumerevoli funzionalità hardware come i timer, i pin PWM, gli interrupt esterni e interni e molteplici modalità di sleep.
- Orologio da 16 MHz. Questo non rende più veloce il microcontrollore, ma abbastanza veloce per la maggior parte delle applicazioni.
- Pin digitali e analogici. Questi pin consentono di collegare hardware esterno alla scheda e sono fondamentali per estendere la capacità di calcolo di Arduino.
- Connettore ICSP per bypassare la porta USB e interfacciarsi direttamente con Arduino come dispositivo seriale. Questo è necessario per riavviare il caricamento del chip se si danneggia e non è più in grado di dialogare con il computer.
- Pulsante di reset per ripristinare il programma sul chip.

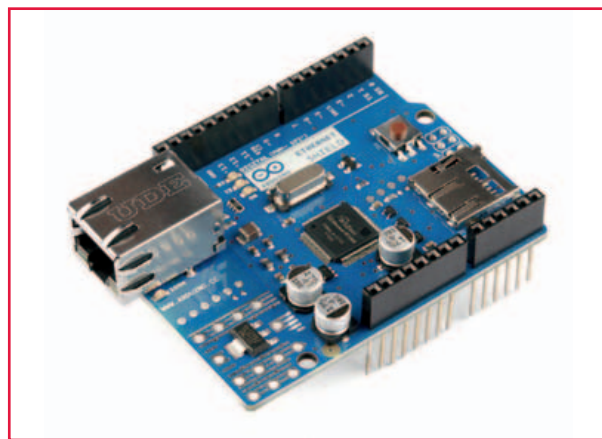



Fig. 4 – Shield Ethernet da collegare alla scheda Arduino UNO

Arduino vs Raspberry

Nella comunità dei maker, non c'è scarsità di opzioni per progettare un sistema di controllo. Due delle opzioni più popolari sono Raspberry Pi, un system-on-a-chip (SoC) che gestisce una versione completa di Linux ed è stato progettato tenendo a mente l'insegnamento della programmazione e dell'elettronica e appunto Arduino con una grande comunità di supporto e centinaia di shield di espansione. Le differenze di specifica tra i due rendono abbastanza ardui i paragoni diretti sulla carta, soprattutto considerando il processore da 16 MHz di Arduino con i 900 MHz del Raspberry Pi. Il Raspberry Pi è un computer completamente funzionale, con un processore dedicato, memoria e un driver grafico per l'output tramite HDMI. Esegue persino una versione appositamente progettata del sistema operativo Linux. Questo semplifica l'installazione del maggior numero di applicativi e consente di utilizzare Pi come un flusso multimediale funzionante o un emulatore di videogiochi. Sebbene Raspberry non disponga di archiviazione interna, è possibile utilizzare le schede SD come memoria flash per l'intero sistema, consentendo di scambiare rapidamente diverse versioni del sistema operativo o aggiornamenti software per il debug. Grazie alla connettività di rete indipendente del dispositivo, è anche possibile impostarlo per accedere tramite SSH o trasferire file su di esso utilizzando FTP. Lo scopo principale della scheda Arduino è interfacciarsi con sensori e dispositivi, quindi rappresenta la soluzione ideale per i progetti hardware dove si desidera semplicemente una risposta veloce a diverse letture del sensore. Purtroppo Arduino, a differenza del Raspberry, non prevede la connettività di rete direttamente nella scheda, ma è possibile averla attraverso shield aggiuntive facilmente programmabili grazie alle librerie che il costruttore mette a disposizione (Fig. 4).

La piattaforma Arduino è stata pensata inizialmente per hobbisti e studenti. Con il passare del tempo si è dimostrata all'altezza delle aspettative rappresentando, di fatto, una scheda di sviluppo per la prototipazione rapida e la progettazione di molte soluzioni definitive grazie alla portabilità dell'hardware e software. Le applicazioni più comuni sono robot, design IoT, acquisizione dati.

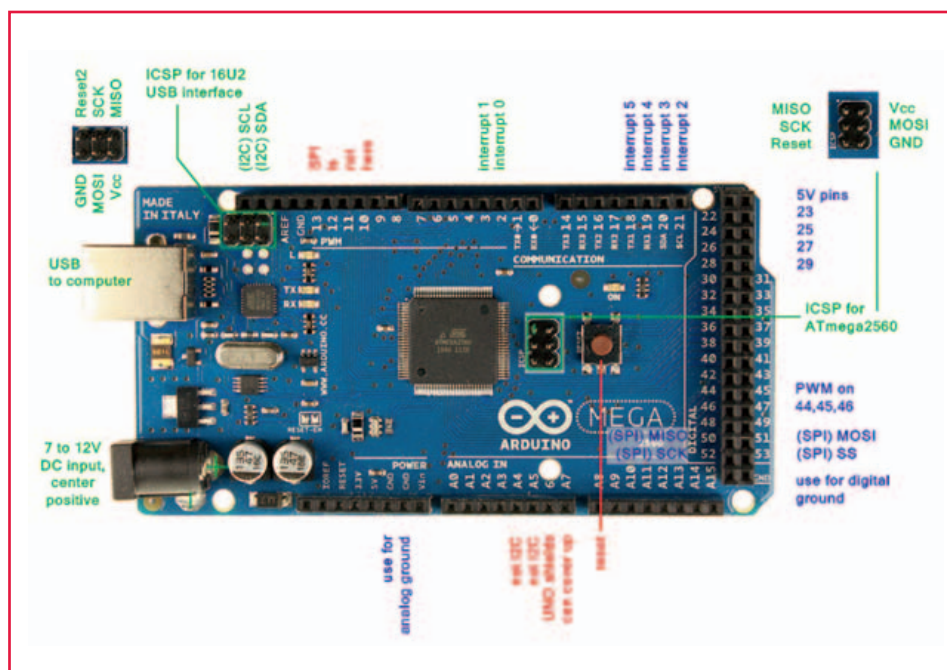



Fig. 5 – La scheda Arduino MEGA con le relative indicazioni dei pin

La flessibilità di Arduino lo rende adatto anche per applicazioni dove è richiesta la connettività di rete al fine di gestire operazioni remote di controllo. Il controllo motore e la gestione di sensori quali quello di temperatura, umidità e accelerometri, rendono la scheda professionalmente appetibile al mondo industriale supportata anche da una grande community per la risoluzioni di problemi.

Il mercato offre tante schede con diverse caratteristiche, in particolare Arduino M0 gestita da Atmel SAMD21, con un core ARM Cortex M0 a 32 bit; LilyPad basata sul microcontrollore ATmega32U4; Arduino Esplora; Arduino Nano con MCU ATmega32u4; Arduino due con processore a 32 bit e Arduino MEGA (Fig. 5).

I sistemi di controllo del futuro

Sfide e tendenze emergenti stanno influenzando i sistemi di controllo distribuito conducendoli verso nuove configurazioni e architetture, alcune già disponibili attualmente, altre nel prossimo futuro

Silvano Iacobucci

In automazione industriale, i sistemi di controllo distribuito (Dcs) rappresentano la soluzione più adottata per i grandi impianti continui (raffinerie, centrali di produzione energia, cartiere, vetrerie, impianti chimici e così via). I Dcs svolgono in modo integrato le funzioni normalmente implementate sui Plc (Programmable Logic Computer) e sui sistemi Scada (Supervision Control And Data Acquisition).

L'architettura tipica di un Dcs comprende vari livelli. Il livello più basso contiene le interfacce verso il campo, costituite da schede di input (acquisizione) e output (comando), e le interfacce di comunicazione per i più comuni fieldbus, attraverso i quali vengono scambiate informazioni con i trasmettitori e gli attuatori che supportano lo stesso tipo di protocollo.

Il livello superiore contiene i controllori, che comunicano attraverso un bus I/O con le schede e le interfacce del primo livello; i controllori elaborano i dati di I/O in base alle strategie di regolazione e alle logiche progettate per la specifica applicazione secondo "blocchi funzione" (ad esempio, un regolatore PID).

Al terzo livello, sopra i controllori, sono presenti i supervisori, implementati oggigiorno su normali PC, che svolgono una funzione di interfaccia per l'operatore di sala controllo, attraverso schermate che rappresentano graficamente l'impianto e i processi. A questo livello si trova anche il database unico e condiviso tra controllori e supervisori, che consente a un sistema Dcs di avere livelli di integrazione molto più elevati rispetto a un sistema composto da Plc e Scada.

Al di sopra dei supervisori, al livello più alto, sono situati strumenti di ottimizzazione, monitoraggio delle prestazioni e gestione della strumentazione e dei macchinari in campo, che sempre più entrano a far parte dello scopo di fornitura di un sistema di controllo distribuito. Anche queste funzionalità vengono espletate da normali pc spesso connessi alla rete aziendale o di stabilimento.

Gli ambienti di processo industriale stanno diventando sempre più complessi e importanti, e al contempo l'industria sta assistendo a una carenza di operatori dotati delle necessarie capacità tecniche. La scelta e l'implementazione di un sistema di controllo distribuito è fondamentale; una strategia efficace può aiutare un'organizzazione a rendere più efficienti i processi con risorse limitate, mentre un sistema Dcs pensato in modo inadeguato può comportare sprechi economici e, in ultima istanza, anche all'abbandono di una produzione.

Le realtà che impiegano il controllo di processo sono notoriamente conservative, data la larga base installata di apparecchiature che spaziano dalla pneumatica a sofisticati sistemi di controllo digitale, che comunque stanno producendo profitti. Quindi mentre sul fronte delle tecnologie commerciali stiamo assistendo a rapidi cambiamenti, l'adattamento dei sistemi di controllo di processo

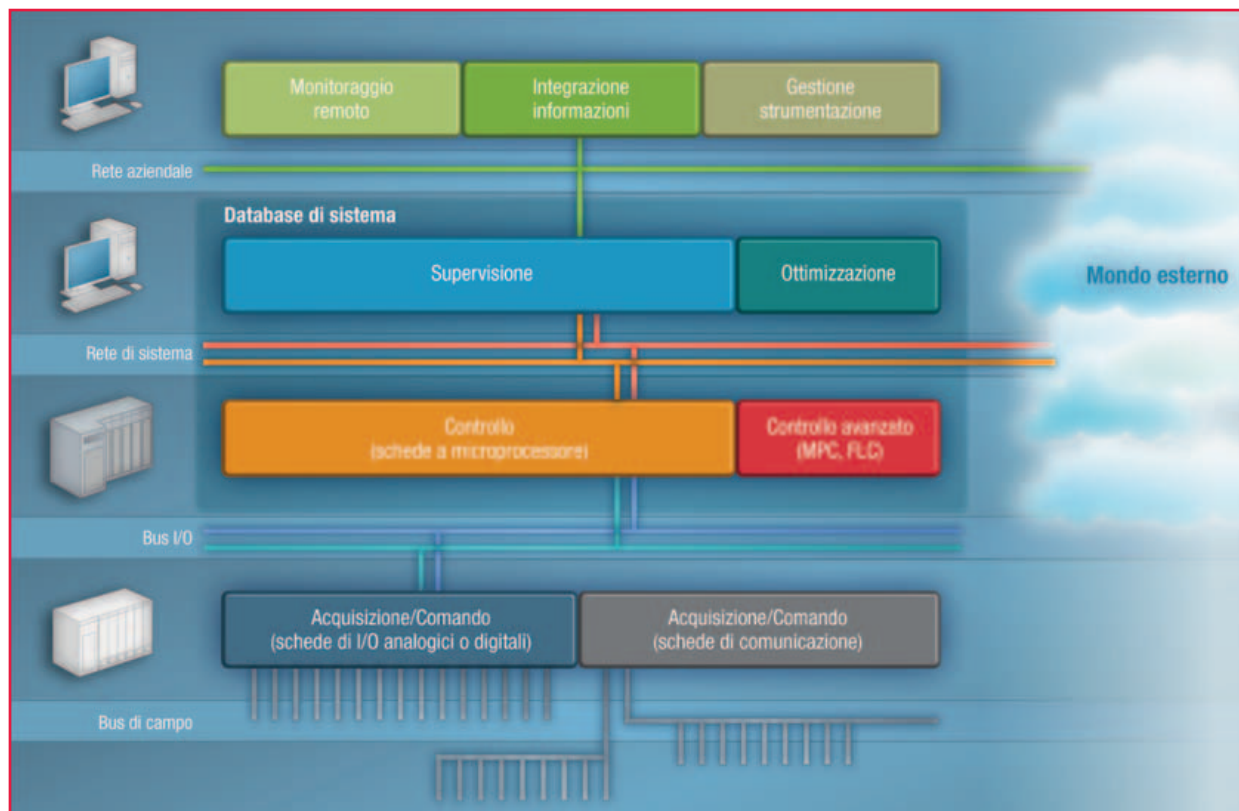



Fig. 1 – Schema architetturale tipico di un Dcs

avverrà secondo il valore aggiunto che le nuove tecnologie permetteranno di acquisire e sull'accettazione "culturale" del personale impiegato. D'altro canto un numero crescente di aziende cercano Dcs in grado di fornire un approccio comune ai loro sistemi che semplifichi il progetto, l'implementazione e l'erogazione del servizio. Per garantire business complessi e di tipo "process-driven", i sistemi di automazione devono diventare sempre più capaci di adattarsi alle modifiche di processo e di mercato in tempo reale e in modo semplice. In primo luogo ci saranno continui miglioramenti incrementali nelle tecnologie dei sistemi di controllo già attualmente disponibili. Molti dei Dcs sono sottoutilizzati e il loro futuro può essere ulteriormente espanso in modo intrinseco o attraverso le offerte dei fornitori. Stiamo anche assistendo a un processo di standardizzazione di tutti i tipi di interfacce e integrazione di componenti, che porterà a sistemi sempre più aperti e interoperabili costituiti da prodotti di fornitori diversi. I sistemi di controllo moderni inoltre vengono dotati di processori sempre più veloci e memorie sempre più capaci, che abilitano a nuove funzionalità quali ad esempio l'integrazione di motori di workflow capaci di incorporare procedure di engineering, produzione e manutenzione. I workflow rappresentano una guida molto importante in fasi operative molto complesse e soggette a errori, come l'avvio o l'arresto di un impianto, e strumenti di ausilio a operatori e manutentori dotati di conoscenze tecniche medio-basse del processo.

Parecchi trend tecnologici e di prodotto hanno comunque già avuto impatti sul mercato dei Dcs e probabilmente lo continueranno a fare nei prossimi anni: I/O più intelligenti e di nuova tipologia, schermi di dimensioni e risoluzione crescenti, maggiore complessità di networking, virtualizzazione, cybersecurity, mobilità, cloud computing, data analytics, intelligenza artificiale, soluzioni a supporto agli operatori, sistemi di sicurezza proattiva. Vediamoli con un maggiore dettaglio.

I/O più intelligenti

Il sottosistema I/O del Dcs ha la responsabilità di gestire centinaia o migliaia di misure di processo differenti e altri input, e inviare comandi di azionamento a numerose valvole, attuatori, mo-

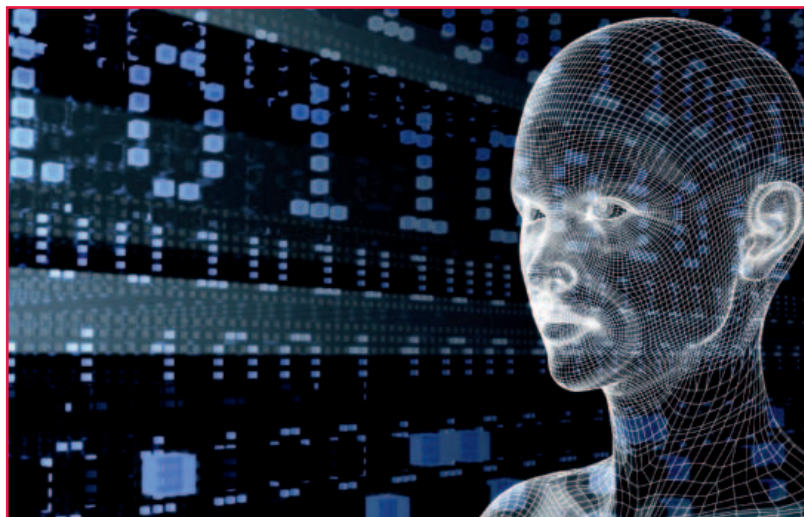



Fig. 2 – Automazione industriale e intelligenza artificiale: un connubio sempre più stretto

tori e altri elementi di controllo dell'impianto. Lo strato di I/O rappresenta una parte significativa del Dcs, e tradizionalmente anche un fattore di costo significativo. I fornitori di Dcs stanno lavorando per ridurre sia il costo e complessità dei dispositive di I/O incorporando più intelligenza e programmabilità al loro interno.

Cambio paradigma di I/O

Una quindicina di anni fa l'input analogico di processo veniva alimentato da un sensore che produceva un segnale 4-20 mA, così come il tipico output analogico.

I segnali discreti comportavano varie combinazioni di tensioni e correnti e ciascun tipo di segnale aveva una scheda dedicata.

Oggi in un impianto nuovo la maggior parte dell'I/O viaggia su alcuni tipi di rete bus, mentre sugli impianti già esistenti è in corso una migrazione dal paradigma 4-20 mA al bus, che risulta più veloce quando nel progetto è compresa anche l'installazione di sensori e attuatori di nuova generazione.

Si sta assistendo anche a una tendenza crescente che prevede l'affiancamento anche di I/O e dispositive wireless, in particolare per applicazioni di monitoraggio di apparati e processo.

Display

Gli operatori disporranno di schermi sempre più grandi (ad esempio schermi singoli da 84 pollici e videowall da 70 metri di lunghezza per 3 di altezza) e ad altissima risoluzione (4 K), in modo da essere visti anche da lontano o contenere grandi moli di informazioni. L'operatore non dovrà più navigare attraverso le schermate per indagare situazioni anomale, ma un sistema intelligente visualizzerà direttamente la situazione guidandolo anche nella ricerca della causa primaria del problema. In alcuni casi i display saranno curvilinei e di tipo touch.

Complessità di networking

Con la scomparsa di una linea di demarcazione tra automazione e IT e con un accresciuto utilizzo di componenti commerciali provenienti da diversi fornitori, la capacità e complessità di interconnessione del Dcs e della architettura di rete dell'impianto si espanderanno. Gli utenti finali di conseguenza dovranno affidarsi sempre più all'esperienza e consulenza di terze parti per installare in modo adeguato e sicuro le reti.

Virtualizzazione

I fornitori di Dcs hanno iniziato a impiegare la virtualizzazione dei server già alcuni anni fa. Gli impieghi comuni di questa tecnologia comprendono lo sviluppo dell'engineering, la simulazione in fase di formazione e la gestione di altre applicazioni off-line.

È invece preferibile usare hardware dedicato al posto di un sistema virtualizzato per controllori di processi real-time dove velocità, determinismo e alta affidabilità sono un imperativo.

Cyber security

Con l'impiego di sistemi open, interoperabili e di mercato, la cyber security sta diventando molto importante anche in relazione ai sistemi Dcs e Scada. La maggior parte dei fornitori ora sta indirizzando questa minaccia con programmi attivi spesso in partnership con terze parti. Deve essere messa in atto una strategia di difesa a 360°, comprendente assessment, architetture, politiche e gestione della sicurezza informatica. Deve diventare comune l'impiego di sistemi di intercettazione e difesa pe-

rimetrale, di firewall di rete e switch in grado di prevenire la propagazione di virus e le intrusioni. Le minacce interne provenienti da PC compromessi o personale malevolo devono essere indirizzate con il blocco delle porte USB e sistemi di monitoraggio dell'attività di rete interna dell'impianto di automazione. Devono essere previste anche delle verifiche periodiche dei livelli di sicurezza attraverso test di vulnerabilità. Inoltre le pratiche di manutenzione della rete e dei sistemi comuni al mondo IT, quali l'aggiornamento software e antivirus, il patching, il bug fixing, devono essere modificate in modo da coprire l'ambiente mission-critical industriale con orari 24x7 in cui i Dcs tipicamente operano.

Mobilità

Proprio come molte persone oggi trovano difficile vivere la quotidianità senza il proprio smartphone, gli operatori di processo e i supervisori della produzione si stanno sempre più basando sulla capacità di accesso da remoto e in qualsiasi orario per svolgere le loro funzioni lavorative. I fornitori di Dcs stanno indirizzando questo trend, che si prevede abbastanza significativo nei prossimi anni, fornendo tecnologia compatibile con tablet e smartphone.

Cloud computing

È plausibile che il cloud computing entrerà a far parte della prossima generazione di Dcs e Scada, anche se il grado di penetrazione di questa tecnologia e il bilanciamento tra i mondi virtuale e hardware-software è ancora parzialmente ignoto e controverso a causa di una realtà molto conservativa.

Data analytics

La Data analytics è la scienza che esamina grandi moli di dati grezzi (memorizzati in sistemi Big Data) allo scopo di trarre conclusioni, trovare relazioni e convertirle in informazioni utili. Ne è un esempio il Data mining. L'analisi predittiva estrae informazioni per determinare pattern che consentano di predire future tendenze e fenomeni.
Nei Dcs la Data analytics può essere usata per estrarre informazioni utili a operatori di impianto, ingegneri, supervisori e manager, o per analizzare video di sicurezza. Una volta che i dati sono estratti ed elaborati, vengono presentati tramite strumenti di visualizzazione grafica adeguati.

Intelligenza artificiale

L'intelligenza artificiale sarà sempre più incorporata nel mondo dell'automazione industriale (Fig. 2). Gli algoritmi di controllo di processo diventeranno sempre più sofisticati, e la prossima generazione di sistemi vedrà controllori e sensori dotati di intelligenza artificiale con funzioni cognitive e capacità di resilienza e "consapevolezza" nel contesto del processo.

Supporto agli operatori

Un trend specifico riguarda la creazione e messa a disposizione degli operatori di soluzioni a supporto della loro operatività. Tali soluzioni comprendono ad esempio ambienti intelligenti con domotica in grado di adattare le condizioni al numero di persone presenti o sedie con aggiustamento automatico al fisico dell'operatore in base a parametri biometrici (al momento esistono già console Dcs che dispongono di due posizioni per l'operatore: seduto o in piedi), che in futuro potranno anche monitorare il suo stato di salute e il suo livello di attenzione. È plausibile che le interazioni dell'operatore potranno avvenire sempre più anche attraverso il parlato usando linguaggio naturale e tecnologia Bluetooth, e attraverso gesti, oltre che con dispositivi touch e tradizionali mouse e tastiera. L'operatore potrà disporre oltre che del sopra citato workflow di supporto, anche di "assistenti" virtuali simili a Siri di Apple.
Infine, l'interazione con l'ambiente potrà essere arricchita anche da soluzioni di realtà virtuale, realtà aumentata e ologrammi.

Sistemi di sicurezza proattiva

Oggi i sistemi di sicurezza sul lavoro sono tipicamente reattivi, e si basano su vincoli di operatività "sicura". In future assisteremo a un crescente utilizzo di sistemi predittivi complementari in grado di anticipare segnalazioni di emergenza basandosi ad esempio sulla storia passata di eventi e incidenti capitati in simili condizioni ambientali e di processo. L'impiego congiunto di intelligenza artificiale e Data analytics saranno impiegati per catturare ed evidenziare condizioni degradate di apparati od operative che potrebbero portare a un potenziale problema di sicurezza, e avvisare proattivamente l'operatore prima ancora che si verifichi l'evento.

Single board computer: aspetti di design

Attualmente, in settori quali la diagnostica medica e il trasporto, i progettisti sono sempre più impegnati a progettare soluzioni in grado di abbinare intelligenza, connettività ed elevate prestazioni a costi, consumi e dimensioni sempre più ridotte: i computer single board sono una piattaforma ideale per un design rapido e focalizzato

Alberto di Paolo

Le soluzioni Single Board Computer (SBC) continuano ad evolversi in termini di potenzialità, contribuendo così ad aumentare la gamma di scelte possibili per i progettisti. Pertanto risulta utile chiedersi quali sono i fattori più importanti nella valutazione e nella selezione di un SBC. Anche se le esigenze di progettazione dovranno variare in base ai criteri dell'applicazione e dell'ambiente di distribuzione, determinate caratteristiche sono comuni in tutte le implementazioni. Poiché i progettisti continuano a perfezionare i loro design e classificare le proprie priorità funzionali, i criteri che andremo ad analizzare possono servire come una base utile per la considerazione e la valutazione delle SBC.

Piattaforma processore

Il nucleo centrale di ogni SBC è la piattaforma di elaborazione applicativa sottostante. Tradizionalmente, la maggior parte delle SBC erano basate su piattaforme x86 e sono state in qualche modo derivate dal fattore di forma tipico della scheda madre del PC desktop, ancora evidente in alcune delle varianti che vengono utilizzate nel mercato (Pico-ITX, Mini-ITX, microATX, EmbATX e altri). Esse vanno da modelli "standalone" a soluzioni impilabili, come PC / 104, e a soluzioni specializzate per l'utilizzo in sistemi rack. Con le piattaforme System-on-Chip (SoC) basate su ARM che diventano sempre più efficaci e in grado di garantire prestazioni e funzionalità di un'architettura x86 a fronte di consumi molto contenuti, un SBC è diventata un'opzione estremamente valida per tutta una serie di nuove e potenziali applicazioni per le soluzioni basate su x86 esistenti (Fig. 1).

Fig. 1 – SBC conforme al fattore di forma Pico-ITX

Fattore di forma

Gli SBC sono disponibili in una vasta gamma di fattori di forma "standard" che vanno via via riducendosi, in termini di dimensioni, fornendo ai progettisti un'ampia scelta per lo sviluppo di applicazioni innovative in grado di sfruttare un livello molto più elevato di potenza di calcolo. Ad esempio, oggi è possibile creare un SBC compatto basato su una soluzione System-on-Module (SoM) con core ARM e connettività 802.11a /b/g/n e Bluetooth 4.0 pre-certificata in un fattore di forma di soli 50x50 mm e altezza variabile da 5 a 7 mm di altezza. Tale SBC è in grado di fornire prestazioni scalabili con CPU quad core di Cortex-A9 SoC con un set completo di periferiche e interfacce integrate, dall'archiviazione (SATA, SD) all'interfaccia utente (fino a quattro display con multi-touch capaciti-

Fig. 2 – Digi International ConnectCore i.MX6UL SBC Pro è un computer di bordo sicuro, pre-certificato, connesso, disponibile in un fattore di forma standard e in grado di garantire un'ampia flessibilità di progettazione

vo). Un tale livello di potenza e flessibilità di calcolo accoppiato con un consumo energetico notevolmente ridotto è disponibile a un prezzo impensabile solo pochi anni fa. La scelta di un progetto SBC basato su un SoM fornisce un percorso di migrazione per l'integrazione diretta dei componenti, garantendo un design della scheda di supporto con maggiori requisiti di personalizzazione in funzione dei volumi e/o dell'applicazione (Fig. 2).

Affidabilità, longevità, disponibilità

Gli SBC sono utilizzati solitamente in applicazioni specializzate e in condizioni ambientali spesso gravose Le prove relative alla temperatura, agli urti e alle vibrazioni connesse con standard specifici di settore garantiranno che il funzionamento affidabili e senza errori 24 ore su 24 della piattaforma. La selezione dei componenti di un SBC è stata concepita anche tenendo conto della disponibilità globale del prodotto sul lungo termine. Ad esempio, un prodotto può essere realizzato interamente utilizzando componenti industriali che contribuiscono naturalmente ad aumentare l'affidabilità, ma anche alla disponibilità a lungo termine dei componenti costituenti. Alcune soluzioni sono costruite sfruttando la scalabilità del SoM ConnectCore 6, un modulo multichip i.MX6 di NXP con connettività wireless integrata che garantisce una lunga durata in ambienti gravosi e la disponibilità a lungo termine per lo sviluppo di soluzioni con Wi-Fi integrato.

Basso consumo energetico

I progetti che utilizzano SBC basati su ARM, anche quelli che sfruttano processori quad-core, possono assicurare un ottimo rapporto tra prestazioni e consumi sia nelle applicazioni mobile che in quelle fisse. I vantaggi di progettazione intrinseci della piattaforma ARM e delle avanzate modalità di risparmio energetico consentono di ridurre al minimo e di ottimizzare il consumo di energia per varie applicazioni, carichi, temperatura e altri criteri specifici. Inoltre rappresenta un valido ausilio nello sviluppo di prodotti che non richiedono un raffreddamento attivo. Ciò riduce la complessità del design aumentando la durata e, soprattutto, l'affidabilità nel tempo.

Connettività

Internet delle cose (IoT) è pervasivo in tutte le applicazioni che coinvolgono i mercati verticali. Le opzioni di connettività inte-

Fig. 3 – Esempio schematico di una implementazione di SBC nel campo medico (Fonte: Advantech)

grate e complete devono essere prese in considerazione e integrate in un prodotto sin dall'inizio del suo ciclo: la connettività Wi-Fi per consentire la configurazione o il servizio di un prodotto, Bluetooth Classic per l'integrazione dei dispositivi utente, Bluetooth Low Energy per sensori a bassa potenza, Ethernet per i casi di utilizzo che prevedono connessioni di rete cablate. La connettività comporta la necessità di garantire sicurezza e attendibilità delal counicazione. La prossima generazione di SBC sarà dotata di funzionalità Bluetooth Low Energy e 802.11a/b/g /n (2,4 e 5 GHz) completamente pre-certificati, con supporto driver per Wi- Fi come WPA/WPA2-Enterprise, connettività cellulare e altre opzioni per assicurare che il dispositivo sia collegato a griglie di elaborazioni più grandi. Infine, grazie a una piattaforma sicura e abilitata al cloud, è possibile costruire prodotti per l'IoT in tempi brevi senza alcuna necessità di sviluppare un'infrastruttura cloud, con tutti i relativi costi e rischi.

Dai dispositivi medici...

Per i produttori dell'industria medica, l'innovazione è un requisito "non negoziabile". La complessità del prodotto, inclusa la necessità intrinseca per la connettività wireless, continua a crescere: per questo motivo è necessario disporre di design efficienti che sfruttino componenti affidabili in grado di ridurre i punti di guasto e supportino i lunghi cicli di vita previsti per il prodotto.
I dispositivi medico/sanitari devono diventare sempre più connessi e garantire elevate prestazioni in aspetti chiave quali la sicurezza dei pazienti e la gestione / monitoraggio dei dati. Le complesse e lunghe approvazioni previste dai regolamenti in vigore comporteranno la necessità di accorciare i tempi di commercializzazione e di focalizzare l'attenzione sulle competenze fondamentali. Una soluzione SBC "ad hoc" svolge un ruolo fondamentale per ridurre il time to market. Di conseguenza, i produttori di dispositivi stanno utilizzando in misura sempre maggiore gli SBC per lo sviluppo di design di dispositivi quali pompe di infusione, ventilatori, defibrillatori cardiaci impiantabili, ECG, terminali a parete, monitor paziente, AED e altro ancora (Fig. 3).

...ai trasporti...

Vista la necessità di garantire elevati livelli di efficienza operativa e di sicurezza, le applicazioni di trasporto richiedono dispositivi connessi e intelligenti sempre più affidabili in grado di resistere a sollecitazioni e vibrazioni di notevole entità. Le soluzioni embedded SBC e SoM svolgono un ruolo chiave nei dispositivi per applicazioni marine, veicoli, ferrovie o aerospaziali. In ambito taxi, queste soluzioni integrate possono contribuire a ottimizzare i veicoli elettrici controllando i componenti del motore, mettendo a disposizione un sistema completamente integrato e di ultima generazione. Negli autobus per esempio è possibile monitorare le emissioni e gestire sistemi di raccolta tariffaria. Su una nave commerciale, invece, possono alimentare sistemi di navigazione e gestire la raccolta dei pesci.

...all'agricoltura

Oggi, gli agricoltori sono in grado di ottimizzare ulteriormente la gestione delle colture, osservando, misurando e adattandosi alla variabilità dei loro raccolti. Ad esempio, i sensori di raccolta delle colture montati su combinatori dotati di GPS possono utilizzare schede SBC industriali robuste, al fine di misurare e analizzare i dati relativi ai livelli di clorofilla, all'umidità del suolo e anche alle immagini aeree e satellitari.
La piattaforma può far funzionare in modo "intelligente" seminatrici a velocità variabile, irroratrici e altre attrezzature agricole per ottimizzare i rendimenti delle colture. La connettività wireless per le reti cellulari e l'integrazione dei sensori con tecnologie quali Bluetooth Low Energy, aggiunge una base di calcolo ad alte prestazioni collegata in tempo reale alle applicazioni in ambito agricolo, garantendo un sensibile incremento del livello di efficienza.

Implementare la comunicazione TSN utilizzando componenti standard

Lo standard Time Sensitive Networking è ancora relativamente giovane ed è necessario un periodo di introduzione di dispositivi che adottino periferiche hardware atte alla corretta gestione delle funzioni richieste: in ogni caso, già ora, è possibile sperimentare le caratteristiche e sviluppare prodotti compatibili con questo nuovo standard utilizzando dispositivi come quelli della famiglia RZ/N1 di Renesas

Arno Stock
Renesas Electronics Europe

L'estensione dello standard IEEE 802.1Q per gli switching Ethernet, catalogato sotto la voce generica "Time Sensitive Networking", consente lo sviluppo di architetture di reti di automazione omogenee a partire dal sensore fino al cloud. Al contrario le soluzioni tradizionali, basate su standard di rete a basso livello, per assicurare un robusto livello di gestione in tempo reale, spesso introducono una serie di significativi livelli di discontinuità nell'architettura di rete. La tecnologia TSN è nata per risolvere questi problemi facilitando il flusso di informazioni tra il livello più basso del sistema in contatto con il campo e i più alti livelli del sistema a livello gerarchico. Oltre a questo gli utenti e i fornitori di strumentazione traggono vantaggio dall'utilizzo di un hardware unificato che offre sia flessibilità sia riduzione dei costi. Un altro punto positivo riguarda una migliore utilizzazione della strumentazione installata e del cablaggio attraverso una gestione condivisa adatta ad una ampia gamma di applicazioni senza i rischi derivanti dalle mutue interferenze.
Data l'importanza e il numero di apparenti vantaggi prima menzionati l'introduzione della tecnologia TSN oggi non è più messa in discussione, le principali differenze nelle strategie riguardano solamente le tempistiche e la sequenza dei passi. Un certo numero di fornitori di apparecchiature industriali è già ora in grado di fornire al mercato i primi prodotti compatibili con la tecnologia TSN e molti altri sono in arrivo.
Una domanda chiave nel caso di introduzione delle nuove tecnologie riguarda l'ampia disponibilità di hardware adatto. Gli standard TSN sono ancora relativamente recenti e la loro implementazione all'interno di dispositivi a semiconduttore richiede tempo. D'altro canto solamente una piccola parte, anche se essenziale, degli standard TSN richiede il supporto di un hardware dedicato. Molte delle funzioni relative ai metodi TSN, ad esempio la gestione della rete, sono basate su algoritmi software che possono essere implementate in modo semplice su qualsiasi hardware.
Oggi i fornitori di prodotti che vogliono implementare le funzioni TSN all'interno dei loro nuovi sviluppi hanno la possibilità di scegliere tra due opzioni principali. La prima è quella di utilizzare dispositivi FPGA che forniscono un elevato livello di flessibilità per implementare le più recenti funzioni in modo rapido, d'altro canto il prezzo per questo tipo di approccio è la somma di tre fat-

tori: il costo relativamente alto di questo tipo di dispositivi, i costi di sviluppo, di testing e di certificazione per le applicazioni basate su FPGA e infine i costi di licenza per le IP che devono essere utilizzate. La seconda è quella di utilizzare dispositivi a semiconduttore disponibili sul mercato e che siano in grado di supportare le funzioni TSN verificate, questo approccio è interessante perché invece di sviluppare il sistema da zero è più sicuro scegliere dispositivi che forniscono le funzioni necessarie e che assicurano la compatibilità con gli standard.

La tecnologia TSN per un sistema di automazione

La richiesta di elementi di rete, in particolare negli switch e nei nodi periferici, varia a seconda delle loro funzioni e della configurazione di rete. L'interfaccia di rete di un PLC o di un computer industriale deve essere più efficiente di quella di un semplice dispositivo periferico. Allo stesso modo gli switch a questo livello devono anche gestire un carico di rete molto più alto di quello che deve essere gestito dai dispositivi che si trovano a livelli più bassi nell'architettura di rete. Questo si riflette nelle caratteristiche minime richieste dai componenti corrispondenti e questo è ancora più importante nel campo dei componenti di rete più semplici, nelle soluzioni di rete semplificate per le tipologie ad anello che possono essere sviluppate utilizzando solamente due interfacce Ethernet per ogni singolo componente.

Il sub-standard TSN offre due metodi principali per le trasmissioni cronologicamente deterministiche: Priorità e pre-emption dei frames (in modalità asincrona) e le comunicazioni controllate a livello di tempistiche inserite in slot di tempo riservate (metodo TDMA, in modalità sincrona). Entrambi i metodi possono essere utilizzati in combinazione. Attualmente, nel campo dell'automazione industriale, ci si focalizza maggiormente sul metodo delle comunicazioni controllate a livello di tempistiche grazie al controllo in tempo reale robusto fornito dallo standard TSN. Questo metodo è ormai ampiamente collaudato sul cam-

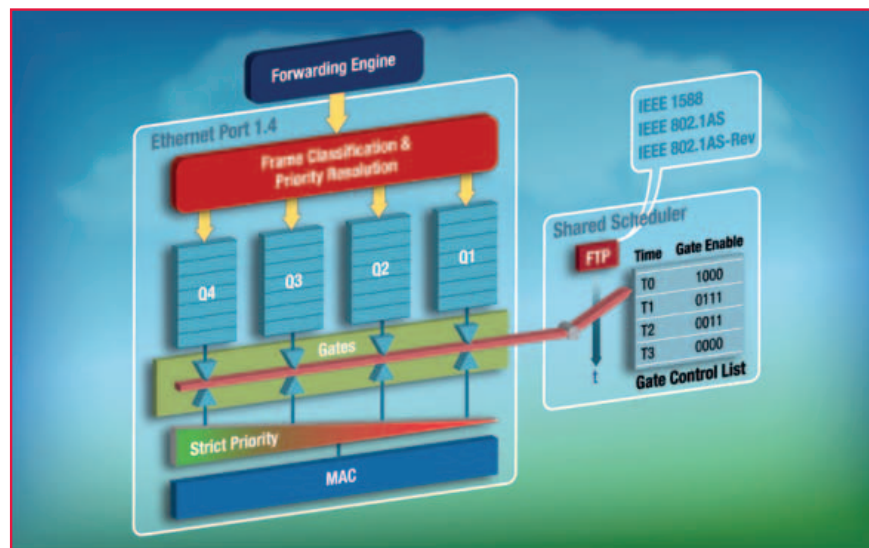



Fig. 1 – Struttura della funzione TDMA

po dato che è quello utilizzato da standard quali Profinet IRT, SERCOS III, EtherCAT e Powerlink. Lo standard TSN IEEE802.1Qbv estende e rende più generici i meccanismi proprietari in modo da espandere il campo delle applicazioni e in modo da abilitare la coesistenza di diversi sistemi che lavorano in tempo reale all'interno dello stesso dominio di rete evitando interazioni multiple.

La trasmissione controllata a livello di tempistiche Qbv evita le collisioni tra differenti flussi di dati lasciando allo switch il ruolo di porta di comunicazione comune. Se il componente di cui parliamo è solamente un nodo con una singola porta di comunicazione Ethernet, ad esempio senza la funzionalità di switch per la ripetizione, in questo caso un controllo preciso delle tempistiche di comunicazione è sufficiente per fare in modo che il componente faccia parte di una rete di comunicazione TSN controllata a livello di temporizzazione. La sincronizzazione con un livello di accuratezza inferiore al microsecondo di tutti i componenti che partecipano alla comunicazione di rete è un prerequisito necessario nelle comunicazioni controllate a livello di temporizzazione. Le procedure stabilite in accordo con le normative IEEE1588 e IEEE802.1AS richiedono le stesse caratteristiche per quando riguarda l'implementazione hardware. I dispositivi corrispondenti devono avere un timer PTP hardware dal quale sono derivate le temporizzazioni sia durante la trasmissione sia durante la ricezione dei messaggi. La frequenza e la fase del timer PTP deve essere modificabile dalla sincronizzazione delle temporizzazioni.

La funzionalità TSN nei dispositive esistenti

Alcuni dei dispositivi attualmente disponibili nel panorama dei dispositivi a semiconduttore, come ad esempio quelli appartenenti alla famiglia Renesas RZ/N1, offrono già ora meccanismi quali la sincronizzazione ad alta precisione e la trasmissione con tempistiche controllate a tempo che utilizzano il metodo TDMA. TSN utilizzerà il nuovo protocollo IEEE 802.1AS che è basato sullo standard IEEE 1588 e che non impone alcuna richiesta aggiuntiva dal punto di vista dell'hardware. La tecnica TDMA è stata anche già implementata

Tabella 1 – Comparazione tra Qbv e Qav +TDMA

Feature	IEEE 802.1Qbv	IEEE 802.1Qav + TDMA[1]
Traffic Queues	8	4
Time Slot	> 8[2]	4
Scheduler	Individual per egress port	Global for all ports
Classification criteria	VLAN PCP, default for untagged frames	VLAN PCP Destination MAC IPv4 (DiffServ) Ipv6 (Class of Service) Programmable Pattern Matcher Ethernet frame type default Queue for untagged frames
Congestion Control	Guard Window	None[3]

1 Usando, come esempio, i dispositivi Renesas RZ/N1.
2 Application-specific, non definiti nello standard QbV.
3 Se necessario un time slot "empty" deve essere inserito e la sua durata deve corrispondere a quella del frame di lunghezza massima

in dispositivi a semiconduttore già disponibili come una estensione delle specifiche Qav allo scopo di assegnare loro uno slot temporale all'interno del ciclo di trasmissione. Questo meccanismo è il precursore del sotto standard Qbv del metodo TSN. Un chip in grado di supportare lo standard 1588/.1AS assieme a Qav + TDMA è adatto per realizzare le funzionalità TSN Qbv più semplici. Questo consente di esplorare i vantaggi della tecnologia TSN in campo a livello di nodi semplici sia per configurazioni a stella sia per configurazioni lineari oppure per configurazioni ad anello.

Fig. 2 – Esempio di Sistema TSN

La Figura 1 mostra la struttura della funzione TDMA all'interno dello schema a blocchi del dispositivo RZ/N1. I frames Ethernet in arrivo, in alto a sinistra, vengono assegnati alle relative porte di destinazione dal blocco hardware denominato "forwarding engine". Qui ogni singolo frame viene classificato a seconda del criterio, configurabile, assegnato ad ognuna delle code (denominate come "Queues"). Il timer hardware gPTP è sincronizzato con la temporizzazione della rete nel dominio TSN. Ogni time slot del meccanismo TDMA è derivato da questa temporizzazione. Ogni time slot, con lunghezza configurabile individualmente, viene specificato in modo centralizzato per tutte le porte Ethernet del dispositivo in una Gate Control List con 4 ingressi. Le code arbitrarie di uscita possono essere aperte in ogni singolo time slot e questo meccanismo è controllato da un sistema di bitmask. In questo contesto "aperto" significa che un frame Ethernet, che è presente nella coda, può raggiungere il MAC, e quindi il cavo di trasmissione, attraverso il controllo di priorità. Il controllo di priorità seleziona sempre il frame Ethernet con il livello di priorità più alto e apre la porta di comunicazione relativa. In ogni caso i frame Ethernet che risiedono nelle code "chiuse" non vengono gestiti all'interno dei time slot rilevanti per la gestione in tempo reale.

Le caratteristiche principali di un hardware compatibile con la struttura Qbv risiede principalmente nel numero di code individuali e nel numero di time slot, ad esempio la differente gestione di ogni singolo frame Ethernet. La tabella 1 mostra una comparazione dettagliata. Per esempio i dispositivi della famiglia RZ/N1 supportano quattro code e quattro time slot. Per vostro riferimento lo standard TNS Qbv definisce otto code e non definisce il numero di time slot. Oltre a questo lo standard Qbv richiede un timer gPTP centrale, la Gate Control List è specifica per ogni porta così che ogni singola porta può avere una gestione temporale individuale.

Per un dispositivo di campo che possiede una sola porta Ethernet e per i dispositivi di campo collegati con linea semplice o ad anello le limitazioni precedenti sono spesso accettabili. Questo perché vengono utilizzati solamente poche tipologie di messaggi in tempo reale e la schedulazione delle trasmissioni di tutte le porte è identico in modo da permettere un flusso ininterrotto di messaggi Ethernet attraverso i vari componenti e quindi attraverso la connessione ad anello. Il seguente esempio di applicazione TSN descrive le affermazioni precedenti.

Esempio applicativo TSN

La configurazione di esempio illustrata in figura 2 mostra come può essere sviluppata una soluzione di automazione, basata su TSN, utilizzando le caratteristiche dei dispositivi Renesas RZ/N1. Un PLC compatibile con lo standard TSN, sia fisicamente esistente nell'impianto sia virtualmente presente su un computer di rete, controlla un gran numero di componenti di ingresso / uscita che sono organizzati in due linee. In alternativa, in questo caso, è anche possibile utilizzare una struttura ad anello. Il traffico di rete è temporizzato e sincronizzato con i cicli funzionali del PLC. I cicli funzionali del PLC si suddividono in tre fasi: Lettura del valore reale dai dispositivi di ingresso / uscita, calcolo dei nuovi valori di uscita attraverso l'algoritmo di gestione del PLC e invio dei nuovi valori di uscita verso i dispositivi remoti. Durante il ciclo di esecuzione la prima e la terza fase si sovrappongono dal punto di vista temporale. La dorsale TSN che consiste negli switch, di tipo TSN, TSW 1 e TSW 2 deve gestire tutto il traffico di rete tra il PLC e gli anelli sottostanti e, ove necessario, come indicato dagli switch TSW x1 e TSW x2, anche il traffico aggiuntivo tra i componenti di rete connessi al segmento in questione. Questo richiede il supporto completo dello standard Qbv di TSN e, quando richiesto, il supporto Qbu per gli switch di dorsale TSW 1 e TSW 2.Le richieste per le sotto linee sono molto più rilassate. I componenti TEP n.m devono solamente trasferire il traffico di rete in arrivo e in partenza da e verso i componenti limitrofi. Il loro ruolo come endpoint TSN è limitato alla ricezione e alla trasmissione di singoli messaggi in tempo reale da e verso il PLC e alla gestione di altre comunicazioni non critiche dal punto di vista delle tempistiche come ad esempio la sincronizzazione del tempo oppure un server OPC-UA. La tabella 2 mostra come, in questo esempio, le differenti classi e la loro mappatura sull'hardware disponibile a bordo dei dispositivi della famiglia RZ/N1 consente di rispondere a tutte le richieste di funzioni TSN. In questo esempio tutti i componenti di rete, gli switch e i nodi sono sincronizzati tra di loro per mezzo del sistema di sincronizzazione del protocollo IEEE 802.1AS e utilizza trasmissioni controllate a livello di temporizzazione per evitare collisioni. Le comunicazioni vengono effettuate all'interno di uno slot di tempo prefissato che si ripete ciclicamente. Per questo tipo di dispositivi, posizionati nelle sotto linee, l'assegnamento delle classi agli slot di tempo è mostrato in Tabella 2. Il ciclo di tempo e la lunghezza di ogni singolo slot dipende dall'applicazione. Lo slot di tempo T3 è sempre vuoto, questo significa che nessuna coda dovrebbe essere inviata durante questo periodo di tempo e dovrebbe possedere la lunghezza del più lungo messaggio che viene trasferito su Ethernet. Questo garantisce che le porte di uscita all'inizio del finestra in tempo reale T0 sono sempre libere e non occupate da messaggi precedenti per evitare di generare ritardi indesiderati durante la trasmissione di messaggi in tempo reale.

Tabella 2 – Classi di comunicazione della rete di esempio

Priority	Class	Example	Queue	T_0	T_1	T_2	T_3
7	Real-time data	I/O data	4	1	0	0	0
5	Network control	Time synchronisation	3	0	1	0	0
3	Prioritised	OPC-UA	2	0	1	1	0
1	Others	http, Status, Diagnosis	1	0	1	1	0

T_0: Time slot for real-time data only. Avoidance of collision with other classes.
T_1: Time slot for all remaining classes
T_2: Time slot for low-priority data only, to ensure minimum throughput.
T_3: Guard band, guarantees a free output port immediately at the beginning of T0 of the next cycle

Cycle				Cn				Cn+1				Cn+2
SPS State				Data I/O	Computing RT.out for tn+1			Data I/O	Computing RT.out for tn+1			
Link (Port to Port)												
SPS/Cloud	E	TSW1	4.I	RT.out.2.tn RT.out.1.tn	Net Ctrl	OPC-UA & Best effort		RT.out.2.tn+1 RT.out.1.tn+1	Net Ctrl	OPC-UA & Best effort		
	I		4.E	RT.in.2.tn RT.in.1.tn	Net Ctrl	OPC-UA & Best effort		RT.in.2.tn+1 RT.in.1.tn+1	Net Ctrl	OPC-UA & Best effort		
TSW1	1.E	TSWx1		Net Ctrl	Other RT	OPC-UA & Best effort		Net Ctrl	Other RT	OPC-UA & Best effort		
	1.I			Net Ctrl	Other RT	OPC-UA & Best effort		Net Ctrl	Other RT	OPC-UA & Best effort		
	2.E	TEP1.n	1.I	RT.out.1.tn	Net Ctrl	OPC-UA & Best effort		RT.out.1.tn+1	Net Ctrl	OPC-UA & Best effort		
	2.I		1.E	RT.in.1.tn	Net Ctrl	OPC-UA & Best effort		RT.in.1.tn+1	Net Ctrl	OPC-UA & Best effort		
	3.E	TSW2	1.E	RT.out.2.tn	Other RT	Net Ctrl OPC-UA & Best effort		RT.out.2.tn+1	Other RT	Net Ctrl OPC-UA & Best effort		
	3.I		1.I	RT.in.2.tn	Other RT	Net Ctrl OPC-UA & Best effort		RT.in.2.tn+1	Other RT	Net Ctrl OPC-UA & Best effort		
TSW2	2.E	TEP2.n	1.I	RT.out.2.tn	Net Ctrl	OPC-UA & Best effort		RT.out.2.tn+1	Net Ctrl	OPC-UA & Best effort		
	2.I		1.E	RT.in.2.tn	Net Ctrl	OPC-UA & Best effort		RT.in.2.tn+1	Net Ctrl	OPC-UA & Best effort		
	3.E	TSWx2		Net Ctrl	Other RT	OPC-UA & Best effort		Net Ctrl	Other RT	OPC-UA & Best effort		
	3.I			Net Ctrl	Other RT	OPC-UA & Best effort		Net Ctrl	Other RT	OPC-UA & Best effort		
TEP1.n	2.E	TEP1.n+1	1.I	RT.in.1.tn	Net Ctrl	OPC-UA & Best effort		RT.in.1.tn+1	Net Ctrl	OPC-UA & Best effort		
	2.I		1.E	RT.out.1.tn	Net Ctrl	OPC-UA & Best effort		RT.out.1.tn+1	Net Ctrl	OPC-UA & Best effort		
TEP2.n	2.E	TEP2.n+1	1.I	RT.in.2.tn	Net Ctrl	OPC-UA & Best effort		RT.in.2.tn+1	Net Ctrl	OPC-UA & Best effort		
	2.I		1.E	RT.out.2.tn	Net Ctrl	OPC-UA & Best effort		RT.out.2.tn+1	Net Ctrl	OPC-UA & Best effort		
		TEP Scheduler		T0	T1	T2	T3	T0	T1	T2	T3	

Fig. 3 – Schedulazione della comunicazione TSN

Schema di comunicazione

Tutti gli endpoint TEP n.m inviano i loro valori reali come variabili di ingresso al PLC all'inizio di ogni ciclo di rete. Il PLC, da parte sua, invia il valore del nuovo stato delle uscite, calcolato dall'algoritmo di controllo, agli endpoint durante l'ultimo ciclo di rete (Fig. 3).
Per questa ragione, in ogni linea della dorsale, lo slot di tempo T0 è riservato e durante questo tempo avviene la trasmissione in tempo reale tra gli endpoint TEP n.m e il PLC. La collisione con altro traffico di rete è quindi impossibile dato che il tempo relativo al messaggio più lungo è garantito. I nodi finali trasmettono il loro valore reale dagli switch TSW 1 e TSW 2 connessi alla dorsale a livello superiore contemporaneamente attraverso entrambe le linee. Questi ricevono i dati e li ritrasmettono al PLC. Anche in questo caso la collisione tra i messaggi che viaggiano sulle linee è escluso perché gli switch di dorsale trasmettono i messaggi di ogni singola rete all'interno di slot separati. Tutto questo richiede la presenza di risorse appropriate a bordo degli switch di dorsale.
I valori in uscita vengono trasmessi in due passi allo scopo di assicurare l'arrivo simultaneo dei valori di uscita del PLC ai nodi TEP n.m, prima la linea 1 e poi la linea 2.
Lo slot di tempo T0 delle sotto linee deve essere calcolato in modo da essere lungo a sufficienza da contenere l'intero frame che rappresenta lo stato di tutte le variabili di uscita. La modifica simultanea dei valori precedenti con quelli nuovi viene eseguita senza il pericolo di incorrere in collisioni di conseguenza non sono necessarie altre misure di controllo e di sincronizzazione per gestire il flusso in direzioni opposte.
Dopo che tutti i valori reali di uscita hanno raggiunto il PLC, all'interno dello slot di tempo assegnato, e dopo che tutti i nuovi valori di uscita hanno raggiunto i nodi finali il PLC esegue il suo algoritmo di controllo che calcola il nuovo valore delle uscite in base allo stato attuale delle uscite stesse e in base agli stimoli esterni e ai comandi di rete. I nodi di uscita elaborano i loro nuovi set point in modo sincrono con le tempistiche definite dalla sincronizzazione di rete in modo da potere modificare lo stato delle loro uscite in modo simultaneo e sincronizzato.
Dopo che il PLC ha eseguito il proprio algoritmo i cicli di rete continuano ad essere gestiti allo stesso modo senza alcuna modifica delle tempistiche di comunicazione assegnate.
Altri dati possono essere trasferiti sulla dorsale TSN al di là degli slot di tempo riservati sia sulla linea uno sia sulla linea due senza preoccuparsi di effetti collaterali nella gestione della rete in tempo reale. Ad esempio i dati in tempo reale (RT x) possono essere incapsulati tra segmenti di rete adiacenti in time slot individuali a patto che sia assicurata la capacità di trasmissione necessaria al corretto funzionamento della rete. Altri importanti flussi di dati aggiuntivi vengono utilizzati per la sincronizzazione temporale della rete oppure per la richiesta di oggetti OPC-UA.

Il posizionamento ad alta precisione entra nel mercato di massa

Per avere successo nelle applicazioni per il mercato di massa, i provider di servizi GPS ad alta precisione non solo dovranno garantire apertura e un'ampia copertura, ma anche essere in grado di introdurre soluzioni innovative capaci di soddisfare le esigenze di applicazioni che richiedono volumi elevati

Peter Fairhurst
Product Line manager
Product Center Positioning
u-blox

Le tecnologie di successo sono quelle che permettono di risolvere i problemi. Si pensi ad esempio alla tecnologia GNSS, ormai presenza costante della vita quotidiana: sono innumerevoli i problemi risolti grazie alla possibilità di conoscere la posizione assoluta di qualsiasi oggetto nel raggio di pochi metri. Oggigiorno, la crescente richiesta di automazione nelle applicazioni di navigazione - dai veicoli altamente automatizzati e autonomi fino alla robotica mobile come i droni - sta facendo emergere la necessità di soluzioni di posizionamento più precise.
Le soluzioni GNSS ad alta precisione esistono ormai da oltre un decennio, e servono principalmente i mercati di nicchia che richiedono prodotti di elevato livello qualitativo. Eppure sono inadatte a soddisfare le maggiori esigenze poste dall'attuale ondata di innovazioni tecnologiche, di cui i veicoli autonomi sono solo un esempio tra tanti. Da un lato, il loro costo, le dimensioni e il peso elevati le rendono poco idonee per numerose applicazioni del mercato di massa mentre dall'altro "pesa" la mancanza di scalabilità - un problema gravissimo per una tecnologia che, da qui a pochi anni, potrebbe rappresentare uno standard per le nuove automobili. Grazie all'hardware dei dispositivi GNSS di nuova generazione e ai servizi di correzione è possibile iniziare a superare queste barriere e sul mercato di massa iniziano ad apparire soluzioni GNSS che abbinano elevata precisione, compattezza dimensionale, costi accessibili e completa scalabilità.

Dalle offerte di ieri...

Per poter beneficiare degli odierni servizi GNSS ad alta precisione sono necessari dispositivi di posizionamento in grado di inviare la propria posizione, seppur approssimativa, a un fornitore di servizi di correzione. Monitorando gli errori del GNSS - in prima linea quelli indotti dalla ionosfera - tramite una rete di stazioni GNSS di riferimento, il provider di servizi è in grado di fornire ogni singolo dato di correzione dei propri clienti, calibrato in base alla posizione specifica dell'applicazione in uso.
I rilevamenti e, più di recente, le applicazioni per il controllo delle macchine e degli strumenti agricoli hanno beneficiato dei servizi di posizionamento precisi al centimetro a fronte di un costo dell'abbonamento annuo di circa 600-1.000 dollari per ogni ricevitore GNSS. Molto costosi, questi servizi operano spesso entro i confini di un solo Paese, talvolta addirittura all'interno di un singolo Stato. Un fattore forse positivo per un contadino sedentario, non certo per altri utenti finali. Si immagini di attraversare il confine di una nazione o di uno Stato con un veicolo connesso oppure di dover effettuare riprese aeree in una regione estera utilizzando un velivolo senza pilota: in questo caso sarebbe necessario districarsi con contratti di roaming o spese supplementari per continuare a beneficiare dei servizi GNSS ad alta precisione una volta giunti a destinazione. A questo punto entra in scena la scalabilità. I servizi GNSS convenzionali ad alta precisione si avvalgono della

comunicazione bidirezionale sulla rete cellulare per trasmettere messaggi tra l'applicazione dell'utente e il provider di servizi di correzione. Mantenere queste condizioni quando migliaia o potenzialmente milioni di dispositivi si contendono la larghezza di banda con altre richieste di dati cellulari renderà difficile, se non impossibile, offrire l'accesso al servizio di correzione. Ciò vale soprattutto per le applicazioni critiche per la sicurezza, dove la perdita di servizi di correzione si traduce in un minor grado di sicurezza per gli utenti - con tutte le implicazioni che ciò comporta.

Fig. A – I dati derivanti da processi di osservazione, identificazione, rappresentazione e correzione richiedono una comunicazione bidirezionale che se da un lato permette un posizionamento ad alta precisione dall'altro rende difficoltosa la scalabilità

… alle prospettive di domani

Attualmente è in atto un cambio di paradigma nel GNSS ad alta precisione, dove un nuovo tipo di servizio di correzione GNSS sta iniziando a consentire di superare queste barriere, in parte neutralizzando l'esigenza di una loro comunicazione bidirezionale con il dispositivo dell'utente finale. Piuttosto che inviare le informazioni relative alla posizione di ciascun dispositivo sugli errori del sistema GNSS, questi nuovi provider di servizi modellano di continuo tutti gli errori rilevanti relativamente a un intero territorio geografico, trasmettendo tali informazioni tramite Internet o il satellite. La tecnologia che si avvale della State Space Representation (SSR) è un esempio di questo nuovo modello di servizi di correzione GNSS. Ciò porta a un ripensamento per l'intero settore. Trasmettendo il dato di errore modellato ai ricevitori GNSS in tutta la regione, piuttosto che supportare individualmente una comunicazione bidirezionale, apre la strada ad applicazioni ad alti volumi destinati ai mercati di massa, "minacciando" allo stesso tempo il modello aziendale dei costosi servizi in abbonamento.

Fig. B – La trasmissione dei dati di correzione GNSS tramite SSR consente di disporre di applicazioni GNSS ad alta precisione per il mercato di massa

L'esempio viene dall'Est

Il Giappone è stato il precursore nella trasmissione di informazioni su errori del sistema GNSS a livello nazionale tramite il satellite QZSS e il segnale L6, fungendo così da banco di prova per le applicazioni del mercato di massa. Benché geograficamente limitato al territorio nipponico, il Centimeter Level Augmentation Service (CLAS) sta già riscuotendo un grande interesse per le applicazioni giapponesi ad alta precisione, ad esempio, nell'agricoltura specializzata, nel controllo di macchine e nella guida autonoma. Nel settembre del 2017, Mitsubishi Electric ha annunciato test di settore sul proprio sistema di guida autonoma, basati sul servizio CLAS. In Cina, QXWZ sta adottando un approccio alternativo ai servizi GNSS ad alta precisione. Piuttosto che avvalersi del broadcasting, QXWZ ricorre a un accesso privilegiato alle proprie stazioni di riferimento GNSS per superare i limiti dell'approccio standard e offrire così ai clienti del territorio nazionale servizi di correzione su misura, rivolti non solo agli utenti finali individuali ma anche agli OEM e agli integratori di sistemi. Nonostante il successo riscosso in Cina, tale soluzione non risulta soddisfacente per gli OEM che operano a livello globale, in quanto obbliga i propri clienti a rintracciare i servizi di correzione GNSS a livello locale. Un nuovo e recente sviluppo è rappresentato dall'avvento di ricevitori GNSS multibanda. Questi potrebbero migliorare la fruizione da parte dell'utente in numerose applicazioni commerciali, fornendo una maggiore precisione nel posizionamento GNSS autonomo. In ogni caso, neppure i ricevitori GNSS multibanda autonomi saranno in grado di fornire la precisione al centimetro richiesta per i veicoli altamente automatizzati e la robotica mobile e sarà comunque richiesto un servizio di correzione.

La prospettiva europea

A livello europeo, i servizi di correzione GNSS sareb-

Fig. C – Il GNSS ad alta precisione consente applicazioni di ampio raggio, tra cui la consegna di merce tramite droni

bero utili sia per i clienti sia per i provider di servizi poiché semplificherebbero l'utilizzo e servirebbero mercati di grandi dimensioni. Ciò è particolarmente vero in un continente come l'Europa dove la mobilità transfrontaliera e l'attività economica sono molto fervide. Sapcorda, una nuova joint venture con sede in Europa costituita da u-blox, Bosch, Geo++ e Mitsubishi Electric sta allestendo un servizio di correzione GNSS di nuova generazione per l'Europa e gli USA, basato sull'esperienza giapponese. Ma invece di avvalersi della comunicazione via satellite, Sapcorda trasmetterà i propri dati di correzione in tutto il continente attraverso la rete cellulare. Piuttosto che "legare" gli utenti a un unico produttore GNSS, Sapcorda renderà disponibili i propri dati di correzione attraverso Internet in un formato aperto, consentendo così a tutti i produttori di hardware di sviluppare le proprie soluzioni GNSS ad alta precisione. Tale approccio sarà una vera "manna" per il settore, in quanto l'accesso ai servizi di correzione da qualsiasi punto del continente trasformerà quello che oggi è un servizio di nicchia in un servizio per il mercato di massa, a favore di veicoli autonomi e semiautonomi e dei droni di rilevamento, ampliando le applicazioni IoT.

Appianare le divergenze

I servizi di correzione GNSS ad alta precisione sono ancora agli esordi - e ci sono varie tecnologie e modelli aziendali che competono per un ruolo di primo piano. Piuttosto che offrire servizi di correzione GNSS agli utenti finali in un formato aperto, il servizio statunitense di Trimble, ad esempio, funziona solo per i dispositivi che utilizzano i loro ricevitori GNSS. Offrendo soluzioni perfettamente integrate, Trimble può garantire l'interoperabilità dell'intera gamma di prodotti - almeno nelle regioni servite da una buona copertura. Tuttavia, gli OEM che vendono a mercati geograficamente diversi tenderanno a rinunciare a tali benefici a fronte di una copertura globale offerta da una serie di provider che utilizzano i dati di correzione aperti. Nelle applicazioni critiche per la sicurezza come la guida autonoma oppure dove la precisione è essenziale per l'intera catena del valore, come il rilevamento mediante droni, la solidità del servizio è un aspetto non negoziabile. Per far sì che le trasmissioni non si "affollino" nel momento in cui le reti cellulari si saturano, ublox si sta impegnando attivamente impegnando, assieme al Gruppo 3GPP, nello sviluppo di standard specifici per meccanismi di diffusione che garantiscano l'osservanza degli accordi sui livelli di servizio. Mentre Giappone e Cina hanno sviluppato una copertura a livello nazionale, nessuno ha ancora provato a espanderla ai servizi ad alta precisione di un intero continente o, addirittura, a livello globale. Se riuscisse nel proprio intento, Sapcorda sarebbe la prima azienda a superare l'ostacolo rappresentato dai confini nazionali e dai provider di servizi mobili nazionali. Resta ancora da vedere come si adegueranno gli odierni provider di servizi.

Customer satistaction: il fattore chiave

Per avere successo nelle applicazioni per il mercato di massa, i provider di servizi GPS ad alta precisione non solo dovranno garantire copertura e apertura assoluta, ma anche essere in grado di introdurre soluzioni innovative che permettano loro di soddisfare le esigenze di applicazioni che richiedono volumi elevati. La soddisfazione dei clienti finali sarà dunque un elemento fondamentale affinché la tecnologia possa diventare accessibile nella sua globalità. Se, ad esempio, i confini nazionali e statali, gli abbonamenti o i regolamenti in conflitto rappresentassero un problema, dovrebbero essere risolti a monte dell'utente finale. È quanto stanno già facendo i modelli aziendali B2B dove, ad esempio, i produttori di dispositivi lavorano a stretto contatto con i provider di servizi di correzione per far confluire il costo del servizio nel prezzo del dispositivo finale. La nuova generazione di servizi GNSS ad alta precisione spianerà la strada a soluzioni di navigazione automatizzate che sono oggi in fase di progettazione. Al contempo comporteranno un radicale cambiamento per l'intero settore industriale. u-blox si sta adoperando per sviluppare l'ecosistema promuovendo la disponibilità di servizi GNSS ad alta precisione aperti e affidabili per il mercato di massa attraverso la collaborazione con Sapcorda. Inoltre, in qualità di provider di connettività e hardware GNSS per il mercato di massa, sta investendo notevoli risorse per cercare di ridurre il costo di possesso.

Alla scoperta dell'hypervisor

Spesso per motivi economici le funzionalità di dispositivi elettronici diversi vengono consolidate su una base hardware comune. Un hypervisor separa le diverse funzionalità a livello software: in questo modo il debug diventa più difficile, ma non per questo impossibile

Rudolf Dienstbeck
Lauterbach GmbH

Hypervisor: i progettisti di software embedded incontrano sempre più spesso questo termine. C'è una frenesia iperattiva su questa tecnologia (notare il gioco di parole). Per esempio, al momento sembra essere un punto chiave di discussione nei segmenti automobilistico, avionico, aerospaziale, ma anche nell'ambito delle tecnologie medicali. In ogni caso possiamo chiederci: che impatto c'è sui cicli di sviluppo e in particolare riguardo al debug? I tool di debug, soprattutto quelli che accedono all'hardware - per esempio i debugger JTAG - hanno una reale necessità di sapere quando nel sistema sotto test si usa un hypervisor. Naturalmente il progettista vuole avere a disposizione un debugger che gli mostri completamente lo stato del sistema embedded, con tutti i componenti come l'hypervisor, i sistemi operativi guest e i processi guest.

Macchine diverse sullo stesso hardware

Come dice Wikipedia: "Gli hypervisor permettono l'esecuzione contemporanea di sistemi operativi guest diversi su uno stesso sistema host". Sono usati per poter eseguire in parallelo attività diverse su uno stesso hardware, e le attività sono così diverse che si usano sistemi operativi differenti per implementarle. Compito dell'hypervisor è far sì che tutti questi sistemi operativi riescano a girare su un solo computer, condividendo fra loro la CPU grazie a tecniche di timeslicing oppure assegnando dinamicamente ogni singolo core ai diversi guest nel caso di ambienti multicore.

Tutti conoscono gli hypervisor su computer desktop grazie a VMWare o VirtualBox. Per esempio è possibile far girare su Windows una o più distribuzioni Linux complete. Altri esempi, usati anche nei sistemi embedded, comprendono Xen, KVM, Jailhouse e QEMU.

Un'applicazione pratica, scelta nell'ambito dei sistemi embedded, potrebbe essere così strutturata: l'obiettivo è ottenere un cruscotto per auto basato su una distribuzione Linux industriale, un sistema infotainment che funziona con Android, il condizionatore che usa FreeRTOS e il

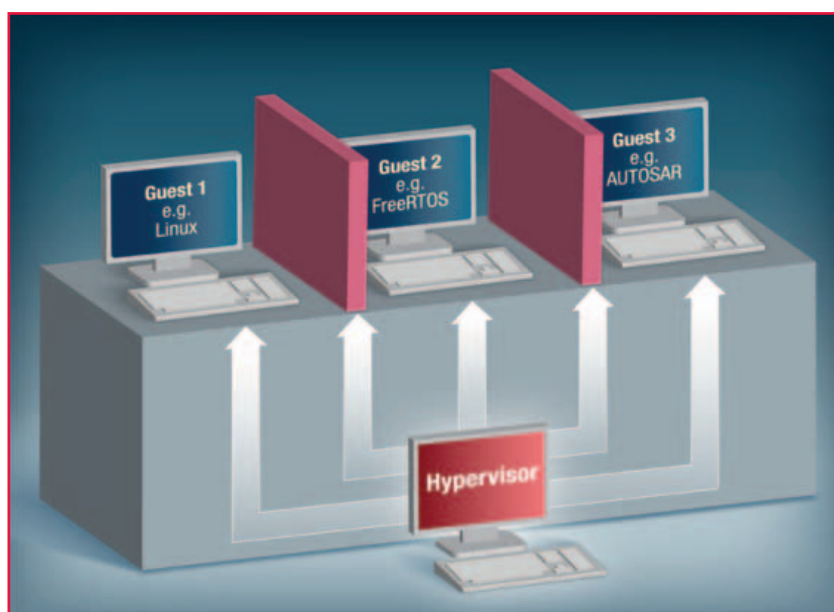



Fig. 1 – Un hypervisor coordina le operazioni di più macchine virtuali su una macchina reale, assicurando una netta separazione fra le macchine virtuali

controllo motore che opera su uno stack AUTOSAR. In passato per ottenere questo scopo sarebbero servite quattro o più piattaforme hardware diverse, ma oggi tutte queste funzioni sono integrate nello stesso sistema e, se possibile, anche nella stessa CPU.

Perché? La prima ragione è legata ai costi. Al giorno d'oggi i sistemi embedded sono così potenti che un solo sistema è in grado di portare a termine tutti i compiti ad esso assegnati. Inoltre è molto più economico produrre e installare un solo modulo hardware integrato piuttosto che quattro sistemi diversi. Questo è il motivo principale, dal momento che ogni centesimo conta, specialmente nell'industria automobilistica. Non dimentichiamo poi che un hypervisor garantisce un ulteriore livello di sicurezza e protezione. L'hypervisor è in grado di monitorare tutti i guest e reagire di conseguenza in caso di malfunzionamenti, per esempio facendo ripartire un guest. È anche fondamentale proteggere i guest da interazioni indesiderate. Un prerequisito di carattere tecnico per ottenere tale protezione è assicurare che tutti i guest rimangano ben separati gli uni dagli altri in termini hardware, mediante un'MMU indipendente (Figura 1). Incontreremo di nuovo questa caratteristica, specialmente quando parleremo di debug.

Fig. 2 – L'hypervisor assicura una completa virtualizzazione del software esistente

Funzionalità dell'hypervisor

In termini hardware i singoli guest possono essere separati fra loro se la CPU permette una completa astrazione dell'hardware. In linea di principio, per ottenere questo risultato devono essere virtualizzate tre risorse: la memoria, le unità periferiche e la CPU stessa (Figura 2). Il sistema operativo guest non dovrebbe neanche essere consapevole che sta girando su una macchina virtuale. Ciò significa che il sistema operativo continua a gestire la propria MMU (MMU di livello 1) e la propria memoria "fisica" (fisica per il guest = intermedia). Ma non si tratta in realtà di memoria fisica. È infatti compilata in un effettivo spazio di indirizzamento fisico grazie a una seconda MMU dell'hypervisor (MMU di livello 2). Anche le unità periferiche vengono virtualizzate (I/O virtuale) per assicurare che ogni singolo guest possa interagire con l'ambiente. È ancora l'hypervisor a decidere quale guest può accedere a quale componente delle unità periferiche, e a quali interruzioni risponda il guest. Infine a ogni guest sono assegnate una o più CPU virtuali che vengono mappate sui core effettivi mediante uno schedulatore. In questo scenario il numero di CPU virtuali di uno specifico guest può essere minore o uguale rispetto al numero di core reali. Riprendendo l'esempio già citato per il sistema automobilistico, una possibile catena di eventi che si potrebbero verificare è la seguente:

- Un sensore di temperatura rileva una caduta al di sotto di 3°C e attiva un interrupt hardware. L'interrupt è ricevuto e processato dall'hypervisor. L'hypervisor inoltra l'interrupt al guest come interrupt virtuale per il cruscotto.
- Il sistema guest riceve l'interrupt virtuale (guest driver) e manda un segnale al processo del guest responsabile per la gestione degli allarmi, il quale stampa "Pericolo: ghiaccio".

Un altro esempio è la comunicazione fra i guest. Il conducente dell'auto si accorge che fuori fa freddo e preme il pulsante del riscaldamento sul cruscotto. Di conseguenza il guest responsabile

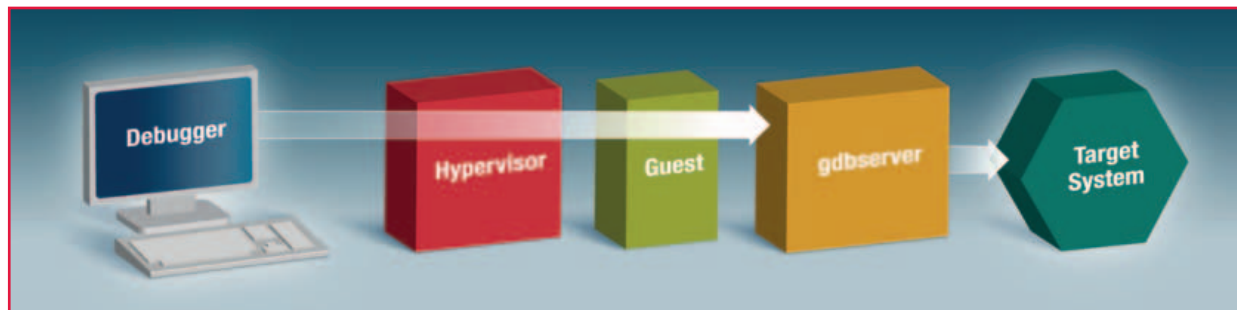



Fig. 3 – Debug "run mode" con gdbserver

per il cruscotto manda un segnale via hypervisor al guest che gestisce il condizionamento, il quale accenderà il riscaldamento.

Impatto dell'hypervisor sui debugger

Finora tutto bene, ma cosa succede se durante la fase di sviluppo il sistema non si comporta come previsto? Ad esempio se la procedura che dovrebbe segnalare l'allarme non si attiva, o se il sistema di condizionamento non capisce cosa vuole l'automobilista? Per trovare la malfunzione è necessario esaminare il software con un debugger.
In teoria ci sono due modalità di debug: il debugging "run mode" controllato a software e quello "stop mode" controllato ad hardware.
Il metodo di debug run mode comporta il caricamento nel sistema di un software di debug aggiuntivo (ad esempio "gdbserver" per processi Linux) che si occupa del debug effettivo. L'avanzamento a step singoli, i breakpoint ecc., sono tutti gestiti da questa unità software, chiamata anche "debug agent". A tal fine un debugger sul computer di sviluppo comunica con l'agent, tipicamente via interfaccia seriale o Ethernet. Per essere sicuri che tutto funzioni vengono fermati solo i componenti sotto debug, ad esempio un processo Linux. Il resto del sistema continua a girare, per questo motivo viene chiamato run mode. Il sistema deve continuare a girare per garantire che la comunicazione con il debugger rimanga attiva.
Questo tipo di sessione di debug ha bisogno solo di un opportuno canale di comunicazione. Se al livello più basso è presente un hypervisor, il canale viene semplicemente ruotato attraverso di esso (Figura 3). Non appena questo percorso è stabilito, né il debugger né tantomeno l'agent sono consapevoli della presenza dell'hypervisor nel mezzo, cioè il debug avviene in modo "hypervisor agnostic". Questo metodo è perfetto se il sistema deve continuare l'esecuzione durante il debug, ad esempio per mantenere attivi dei protocolli di comunicazione. È del tutto sufficiente per il debug delle funzioni di un processo o in caso di processi all'interno di una stessa macchina. Ma questo metodo rivela i suoi limiti quando si entra nel merito dei driver (moduli di Linux), specialmente quando l'utente deve uscire dalla macchina virtuale e sono coinvolti altri guest o l'hypervisor. Se c'è un errore nel segnale di allarme al di fuori del processo nella suddetta catena di eventi, si rende quindi necessario un altro metodo di debug.

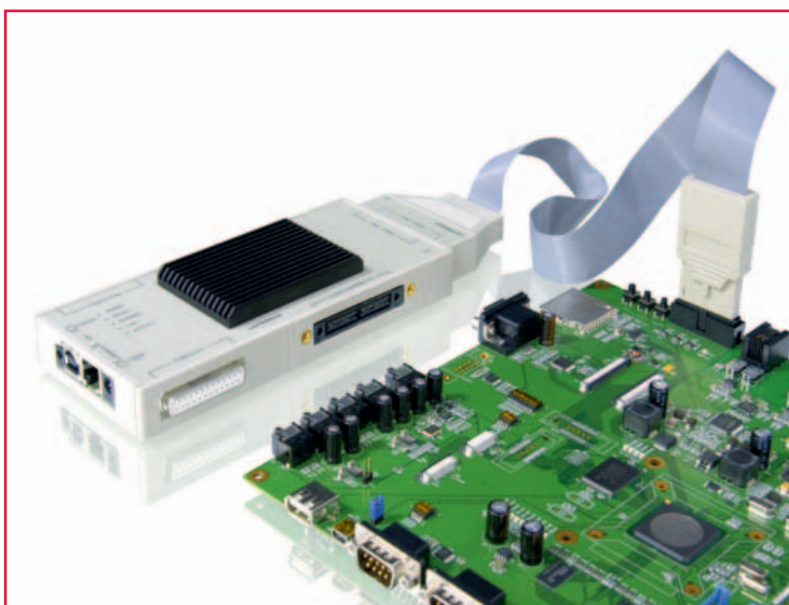



Fig. 4 – Debugger JTAG con sistema target. Questo è il modo in cui un debugger hardware si collega a un sistema target

B::TASK.List.MACHINES

magic	name	mid	access	vttb	extension (s)
	Xen	0.	HD:		Xen
000080007FF51000	Dom0	1.	NUD:	000100007AEF8000	Dom0
000080007AED8000	Linux	2.	NUD:	0002000079FB0000	Linux
0000800079F76000	FreeRTOS	3.	NUD:	0003000079F4E000	FreeRTOS

Fig. 5 – Il debugger "conosce" l'hypervisor e le macchine guest

Debug "stop mode": si ferma tutto

Quando si passa al debugging controllato ad hardware, il debugger è collegato direttamente alla CPU mediante opportuni pin (Figura 4). Il debugger fa uso di questi pin, tipicamente JTAG, per controllare la CPU stessa, per esempio fermandola, attivando singoli step di programma, leggendo i registri o la memoria. Tuttavia ciò significa anche che l'intero sistema, compresi tutti i processi, i guest e naturalmente l'hypervisor, vengono fermati quando scatta un breakpoint. In questo modo non vengono serviti più gli interrupt, non girano più i protocolli di comunicazione e non si hanno più cambi di macchina virtuale, di processi o di task. La CPU è effettivamente ferma, per questo si chiama stop mode.
Quando si trova in questo stato la CPU "vede" solo i componenti attualmente aperti via MMU, cioè un solo guest (quello che sta girando al momento nella CPU) e un solo processo (quello attivo al momento nel guest). Tutti i registri e gli accessi alla memoria fanno riferimento a questo contesto. La CPU non ha alcun accesso ad altre macchine virtuali o ad altri processi. Anche un debugger hardware accede al sistema tramite la CPU e pertanto all'inizio è soggetto alle stesse restrizioni: può solo "vedere" la situazione corrente. Però è capace di fare molto più di questo. Grazie a piccole modifiche temporanee nei registri di MMU, può anche leggere direttamente lo spazio di indirizzamento fisico e l'attuale spazio di indirizzamento "intermedio" (fisico per il guest). Ma tutti i simboli di debug che appartengono ai processi e ai guest sono relativi a indirizzi virtuali e ciò significa che questa vista aggiuntiva non è molto utile per cominciare. Inoltre gli sviluppatori vogliono vedere tutto: l'hypervisor, tutti i guest e tutti i loro processi, tutto quanto e tutto insieme! Questo certamente non si può fare in run mode per i motivi sopra citati, ma si può fare in stop mode e questa è la vera forza di tale metodo. Perché il debugger possa vedere tutto, al di là dello stato corrente, è necessario che abbia una maggior conoscenza del sistema, cioè dimostri una "consapevolezza" (awareness). Servono una "hypervisor awareness", una "OS awareness" per ciascun guest e una "MMU awareness" sia per l'hypervisor sia per ciascun guest, tutti elementi che possono variare in modo considerevole. Poiché il debugger è ora consapevole della struttura del sistema, può leggere la lista dei guest e dei processi, come pure le loro tabelle MMU di sistema. Forte di questa conoscenza il debugger può eseguire la "MMU table walk" (traduzione degli indirizzi virtuali in indirizzi fisici) per ciascun indirizzo virtuale di un guest o di un processo, cioè superare l'MMU hardware e leggere i rispettivi dati direttamente dalla memoria fisica. È proprio implementando questo metodo che il debugger può accedere a tutti gli indirizzi che appartengono a tutti i guest e a tutti i processi, senza preoccuparsi se essi siano virtuali, intermedi o fisici. E tutto questo viene fatto contemporaneamente!

Il debugger ha bisogno di una "awareness"

Così il debugger riesce ad accedere a un sistema target composto da un hypervisor e da più sistemi operativi guest. Ogni macchina ha il proprio set di registri, traslazioni MMU, processi, simboli, breakpoint, ecc. Il debugger deve essere in grado di operare con ciascuna di queste macchine, e questo si applica sia alla macchina "reale" (l'hypervisor) sia a tutti i sistemi guest virtualizzati, come se fossero macchine reali. Naturalmente deve saper operare su tutte le macchine contemporaneamente. Per questo scopo si usa la sopra citata awareness. Una hypervisor awareness deve essere predisposta in modo dedicato per ciascun hypervisor e determina

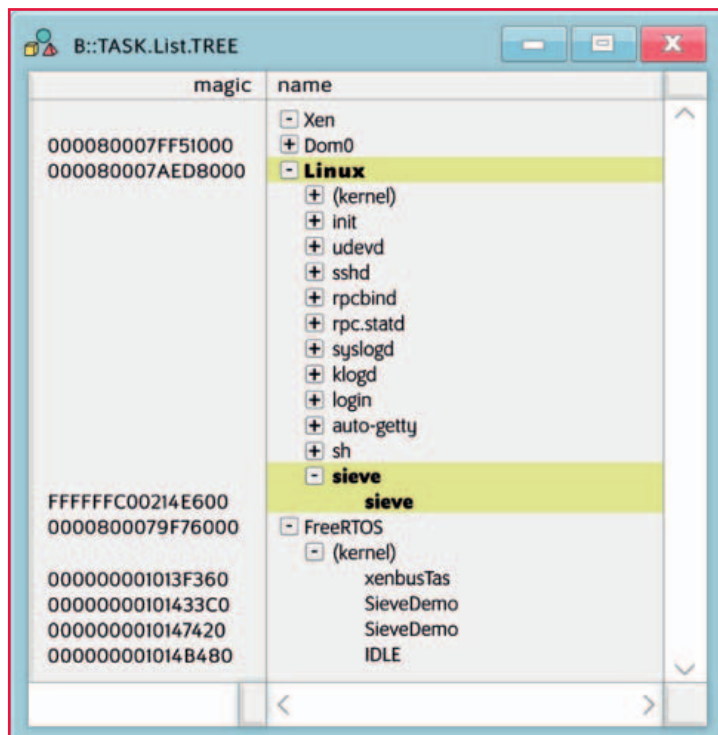



Fig. 6 – Una rappresentazione ad albero mostra la struttura del sistema target

la lista delle macchine virtuali, i loro identificativi, le CPU virtuali e le impostazioni MMU associate. L'awareness utilizza le informazioni simboliche di debug dell'hypervisor (ELF/DWARF) per leggere le necessarie informazioni dal sistema. Una vista delle macchine virtuali con le loro risorse permette di ottenere una rappresentazione eccellente del sistema (Figura 5). L'hypervisor awareness si occupa anche di gestire la struttura delle traslazioni MMU di livello 2, così che il debugger possa accedere a tutte le macchine virtuali.

Per poter analizzare il contenuto di un sistema operativo guest è necessaria una OS awareness, ed ogni guest ne richiede una propria. Anche questa awareness è progettata specificamente per ciascun OS qui utilizzato. Con questa awareness si determinano i processi del sistema operativo e le impostazioni MMU all'interno della macchina virtuale, come pure la struttura delle tabelle MMU (traslazione di livello 1). A tal fine l'awareness utilizza le informazioni simboliche di debug che appartengono al corrispondente sistema operativo, per esempio “vmlinux” quando si usa Linux. In questo modo possono essere visualizzati processi, thread ed altre risorse. Grazie a queste awareness, in ultima analisi il debugger ha una conoscenza delle macchine, dei sistemi operativi e dei processi che girano nel sistema target. Così il debugger TRACE32 sviluppato da Lauterbach è in grado di visualizzare una struttura gerarchica ad albero dell'intero sistema. Su una certa macchina o su un certo processo si possono usare specifici comandi e aprire finestre. Ad esempio si possono vedere contemporaneamente un processo che opera su una macchina Linux e un task eseguito su un dispositivo con FreeRTOS (Figura 6). La gestione dei simboli in TRACE32 è stata modificata opportunamente in modo che lo sviluppatore possa assegnare i simboli caricati a una certa macchina o a un certo processo. È stata anche estesa con un identificativo di macchina (machine ID) e uno di processo (process ID) per far sì che il progettista possa anche accedere sempre a qualunque indirizzo virtuale. In questo modo nessun indirizzo virtuale risulta ambiguo. Se il software passa per un breakpoint l'intero sistema verrà fermato come sopra descritto. Poi il debugger commuta automaticamente sul core (reale) e mostra la macchina e il processo su cui il breakpoint è scattato. Ciò permette all'utente di vedere immediatamente le condizioni che hanno portato a questo break. La macchina virtuale in cui tutto questo è avvenuto viene detta “macchina corrente”, ma naturalmente è possibile cambiare la vista in modo manuale verso gli altri core con le loro “macchine correnti”.

Accesso a sistemi guest inattivi

Con un approccio come questo l'utente non solo può cambiare vista verso altri core hardware, ma può anche passare ad altri sistemi guest al momento inattivi. È quindi sempre possibile accedere ai simboli di tutte le funzioni e le variabili di altre macchine. Le informazioni simboliche erano state caricate per una specifica macchina. Il debugger traduce gli indirizzi virtuali dei simboli in indirizzi fisici (esegue lui stesso la MMU table walk) e, per esempio, va a leggere il valore di una variabile dalla RAM fisica. Durante questo accesso è importante che lo stato della CPU non venga mai

modificato e che tutto sia eseguito all'interno del debugger. Accedendo ai simboli di tutte le macchine, è anche possibile impostare breakpoint su qualunque funzione di qualsiasi macchina in ogni momento. Naturalmente la vista del debugger può essere anche girata verso il set di registri di una certa macchina o di un certo processo. Se in quel momento i registri non sono caricati in un core reale, il debugger ne legge i valori dall'hypervisor o dalla memoria del sistema guest. Con questi valori il debugger determina lo stack frame corrente per mostrare, ad esempio, l'attuale gerarchia di chiamate delle funzioni di un task. Così il progettista può vedere direttamente a che punto è arrivato il task e perché potrebbe essere fermo in attesa.

Fig. 7 – Gerarchia di chiamate di un task inattivo in un guest inattivo

Come si possono usare tutte queste funzionalità per il debug dell'applicazione citata all'inizio? Non dimentichiamo che il processo guest non aveva ricevuto un interrupt hardware. Di fatto ora è facile analizzare questo problema: per mezzo del debugger hardware basta impostare un breakpoint direttamente sul vettore di interrupt. Il sistema si fermerà non appena l'interrupt scatta. Dato che il debugger conosce tutti i componenti, lo sviluppatore ora può seguire la catena degli eventi, cioè l'avanzamento dal punto dell'interrupt nell'hypervisor, attraverso il sistema operativo guest fino al singolo processo, per step successivi o mediante breakpoint sulle diverse fasi. In questo modo è facile trovare qualunque malfunzionamento che potrebbe essere subentrato. Occorre anche dire, però, che le condizioni di stallo sono più difficili da identificare se, per esempio, due processi che comunicano fra loro si bloccano reciprocamente. In questo caso può aiutare la vista di sistema poiché gli stati di tutti i componenti d'interesse possono essere rappresentati vicini fra loro. Pertanto è facile vedere quale task di quale guest - o anche dell'hypervisor - si trovi in uno stato errato o sia potenzialmente in attesa di mutue risorse. Non va sottostimata l'opzione di un'analisi post-mortem se l'intero sistema si porta in uno stato in cui non risponde più. Dal momento che un debugger hardware non richiede alcun software attivo sul sistema target, ci sono le condizioni per analizzare lo stato di tutti i componenti. Grazie al fatto che TRACE32 di Lauterbach contiene anche un simulatore del set di istruzioni, lo sviluppatore può ottenere un dump completo di memoria dal sistema sotto test e analizzarlo comodamente in seguito nel simulatore senza più bisogno del target hardware vero e proprio, come si analizza un core dump. Questa volta però su tutto il sistema, compresi l'hypervisor, tutti i guest e i processi.

Costi più bassi, maggior complessità

Nel mondo embedded si stanno usando sempre di più gli hypervisor. Vantaggi come la riduzione dei costi e il controllo in tempo reale costituiscono chiare argomentazioni a loro favore. Ma questo si paga con il prezzo di una maggiore complessità del sistema. L'hardware deve fornire una virtualizzazione tramite una gerarchia MMU a due livelli che deve essere gestita dall'hypervisor. Un debugger con supporto hardware (ad esempio via JTAG) richiede una conoscenza dell'hypervisor e del sistema guest per poter offrire allo sviluppatore delle viste sul software. Per questo un "awareness" adattata al rispettivo hypervisor e al rispettivo sistema operativo guest deve essere caricata nel debugger, che legge dal sistema target le informazioni necessarie.
Per dimostrarne le funzionalità, Lauterbach ha creato un'implementazione di riferimento con l'hypervisor Xen e i guest Linux e FreeRTOS su una scheda Hikey. Il supporto MMU implementato nel debugger TRACE32 e un'espansione della modalità di gestione degli indirizzi per i sistemi virtualizzati permettono di accedere in ogni momento a qualsiasi componente, così da rendere possibile il debug dell'hypervisor, dei sistemi operativi guest e di tutti i processi guest. Allo stesso modo è anche possibile l'analisi retrospettiva di un'immagine di memoria senza qualsivoglia tipo di problema. Soprattutto lo sviluppatore si ritrova un tool che può usare per debuggare senza sforzo questi sistemi così complessi.

Sistemi operativi real-time: il modello open source fa sempre più strada

I dati emersi da una recente indagine a livello globale sugli utenti evidenziano che il paradigma del codice sorgente liberamente accessibile si estende sempre più anche al mondo degli RTOS. Sistemi operativi come FreeRTOS ed Embedded Linux risultano nelle prime posizioni tra i prodotti scelti dagli sviluppatori nei propri progetti embedded

Giorgio Fusari

Non è soltanto la diffusione delle tecnologie di automazione industriale nel mondo che porta all'utilizzo dei sistemi operativi RTOS (real-time operating system), ma è anche l'aumento di complessità di numerose applicazioni embedded, che, oggi, stimolate da innovazioni come il cloud, la Internet of Things (IoT), l'analisi dei big data, stanno diventando sempre più connesse, guidate dalle informazioni, e dipendenti da processi elaborati in parallelo. Contesti in cui l'utilizzo di un RTOS può risultare vantaggioso, per la precisione di controllo dei task e il funzionamento deterministico, rispetto ai normali sistemi operativi "general-purpose" (GPOS), largamente diffusi in molte applicazioni commerciali. Adattarsi ai nuovi contesti d'uso per gli RTOS significa anche rispondere di volta in volta a esigenze di ottimizzazione estrema dell'utilizzo delle risorse hardware disponibili (cicli del processore, consumo di energia), soddisfacendo al contempo requisiti di isolamento dei processi tramite kernel di separazione, e requisiti di scalabilità, flessibilità, riconfigurabilità, affidabilità, certificabilità, solo per citarne alcuni.

Fig, 1 – Il sistema Amazon FreeRTOS, disponibile sul cloud di AWS
(Fonte: sito web Amazon)

Negli ultimi cinque anni (2012-2017), l'utilizzo di qualche tipo di RTOS, sistema operativo o "scheduler" nei progetti embedded in essere è stato abbastanza costante, come rivela una recente survey condotta dal gruppo Aspencore a livello globale (Stati

Uniti, Canada, Europa, Asia, Sudamerica, Africa e Medio Oriente, Australia), per sondare lo stato dei diversi mercati embedded nel 2017. Tra gli interpellati sull'uso di RTOS, l'86% di quelli che non li adotta dice che la ragione principale è perché, semplicemente, non ne aveva bisogno: in effetti, una prima sfida tecnico-strategica che uno sviluppatore deve affrontare è valutare il tipo di applicazione e decidere se usare o meno un RTOS; quindi stabilire se le sue funzionalità sono realmente necessarie, oppure è possibile ricorrere a qualche tecnica di simulazione dei meccanismi di scheduling dei processi (preemptive scheduling). Per determinare tale necessità, vanno soppesati vari aspetti: ad esempio, si deve comprendere quanto il sistema embedded in questione potrà trarre vantaggio da una gestione più precisa e accurata del tempo di esecuzione dei task, e in che misura un comportamento deterministico sarà realmente necessario nell'economia di esecuzione dell'applicazione. Ma occorrerà valutare anche la capacità di supporto fornita dalle MCU (microcontroller unit) a livello hardware. E da questo punto di vista il superamento del problema potrebbe essere facilitato dal fatto che il progetto embedded preveda l'integrazione di MCU più moderne, con architettura a 32 bit.

Fig. 2 – Il sito web del progetto OpenIL, una piattaforma open source con funzionalità real-time (Fonte: sito OpenIL)

Sistemi operativi commerciali: i costi ne scoraggiano l'uso

Un punto chiave emergente dalla ricerca Aspencore è la diminuzione dell'utilizzo dei sistemi operativi commerciali: nel 2017 dice di usarli il 30% dei rispondenti, rispetto al 40% del 2012. Il 41% usa SO open source, una percentuale che nel 2012 corrispondeva al 31% .

Alla domanda su quali sono i fattori che hanno maggiormente influenzato la decisione di adottare nel proprio progetto embedded un sistema operativo di categoria commerciale, al primo posto (45% dei rispondenti) si posiziona la capacità di funzionamento "real-time". Per contro, a sfavorire l'uso dei SO commerciali si erge l'ostacolo del fattore economico: quando si domanda quali sono i motivi per cui non si è scelto di usare un sistema operativo commerciale, subito dopo coloro (68%) che ritengono che la soluzione in essere funzioni già a dovere, il 35% risponde che queste soluzioni commerciali risultano troppo costose. Ancora, a far comprendere meglio in che direzione stia oggi muovendosi il settore embedded, è il punto in cui si chiede quali sono i più importanti fattori che hanno condizionato la scelta di un sistema operativo: al primo posto (39%) viene messa la disponibilità di codice sorgente, subito seguita (30%) dalla possibilità di evitare il pagamento di royalty. Risposte perfettamente coerenti con quella che poi si rivela la scelta finale del sistema operativo: alla richiesta di fare una selezione di tutti i SO che si stanno attualmente utilizzando, Embedded Linux si colloca al primo posto (22%), seguito da FreeRTOS (20%). Molti altri RTOS commerciali di primo piano si posizionano decisamente più in basso nella classifica.

Tra l'altro il sistema FreeRTOS è attualmente disponibile anche sul cloud AWS (Amazon Web Services), con la denominazione di "Amazon FreeRTOS", e viene proposto come un sistema operativo destinato ai microcontroller dei dispo-

sitivi IoT (Internet of Things), studiato proprio per semplificare lo sviluppo, la securizzazione, l'implementazione e la manutenzione degli "edge devices" basati su MCU. In sostanza Amazon FreeRTOS estende il kernel di FreeRTOS aggiungendo librerie che abilitano e semplificano la connettività locale e nel cloud, mantenendo i requisiti chiave di sicurezza su ciascuna comunicazione.
In linea con queste tendenze, e con l'obiettivo di aprire sempre di più l'accesso alle tecnologie real-time, è arrivato l'annuncio, lo scorso novembre, da parte di NXP Semiconductor, di una distribuzione Industrial Linux con estensioni real-time (framework Xenomai) del SO, e supporto TSN (time-sensitive networking) per l'automazione di fabbrica. La distribuzione "community-based" si chiama OpenIL (Open Industrial Linux) e si propone di abbattere le barriere dell'elaborazione real-time, traghettando gli OEM nell'era del paradigma Industria 4.0 che digitalizza la produzione. La distro OpeIL, ha sottolineato Dan Mandell, senior industry analyst di VDC Research Group, focalizza gli sviluppatori Linux in modo specifico sulle opportunità nel settore dell'automazione industriale, sfruttando al contempo le funzionalità del SoC (system-on-chip) Layerscape LS1028A di NXP per abilitare il modello Industry 4.0 nei sistemi di smart manufacturing. I responsabili dei sistemi di fabbrica e i costruttori di attrezzature industriali, si sottolinea, si stanno orientando verso Linux per la sua stabilità operativa, per la sicurezza che offre e per i vantaggi in termini di costo di possesso (TCO). Per ragioni simili, essi stanno migrando verso lo standard Ethernet, per sostituire i protocolli di networking proprietari e specifici di determinati vendor.

Diversi livelli di requisiti tecnici

Un caso tipico in cui un RTOS può rivelarsi utile è la progettazione di un'applicazione ACC (adaptive cruise control), ossia un sistema di controllo adattivo della velocità di crociera di un autoveicolo. I sistemi ACC sono implementabili utilizzando un sistema di controllo a ciclo chiuso (closed-loop control system - CLCS), in cui i segnali di feedback alimentano di continuo l'applicazione, al fine di correggere in tempo reale la velocità. Qui ogni valore in output in uno specifico momento dipende dall'input ricevuto in quel momento, e occorre assicurare che il dato in ingresso nel sistema sia ricevuto in tempo, affinché venga generato il corretto valore in uscita. I requisiti degli RTOS variano comunque molto in funzione del tipo di applicazione: nella gamma di sistemi operativi classificabili come RTOS sono in effetti presenti diversi tipi di prodotti: nel segmento dei SO di fascia alta, esistono RTOS "industrial-grade", studiati per rispondere a requisiti di funzionamento di tipo "hard real-time" e "safety-critical". Si tratta ad esempio di SO usati in applicazioni avioniche, militari o medicali, in cui il mancato rispetto delle rigide deadline di esecuzione dei processi causa effetti catastrofici sulle cose o sulle persone.
In un altro segmento si collocano gli RTOS "commerciali", in genere usati per soddisfare requisiti di tipo "soft real-time", nelle applicazioni in cui è possibile tollerare una limitata degradazione delle prestazioni nel comportamento deterministico del sistema: si pensi, ad esempio, al funzionamento di un'applicazione

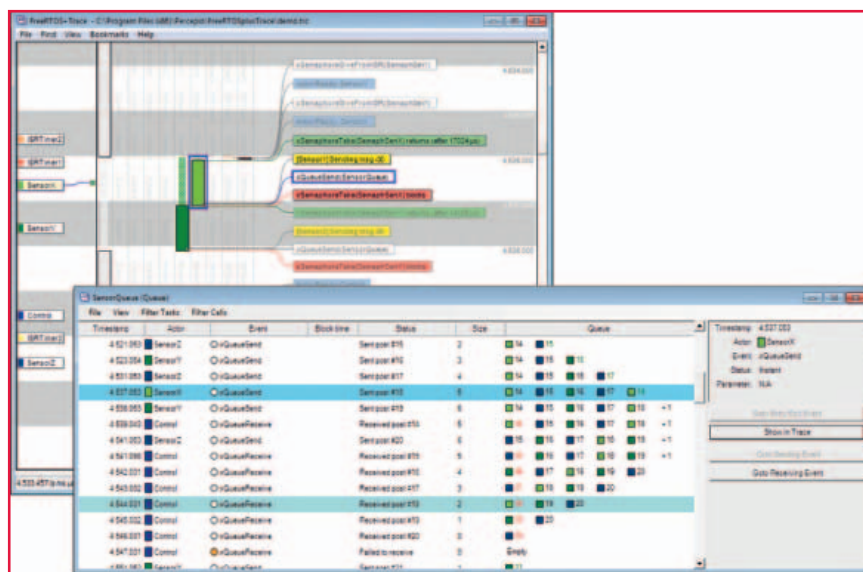



Fig. 3 – Uno screenshot di un tool diagnostico disponibile per il sistema operativo FreeRTOS (Fonte: sito web FreeRTOS)

di gestione audio o video, dove la perdita di qualche bit o frame non pregiudica necessariamente la qualità del servizio o il risultato finale.
L'entità dei danni causati dal mancato rispetto dei requisiti di funzionamento può essere molto diversa: una cosa sono i danni all'incolumità fisica del conducente di un'auto in un incidente stradale, se l'airbag si apre troppo tardi, o anche troppo presto; un'altra sono le perdite economiche e il calo d'immagine che un'azienda subisce, se in fabbrica il sistema d'ispezione automatica della validità di ciascuna parte e componente che procede verso la linea di assemblaggio non compie le proprie operazioni di analisi rispettando i corretti requisiti di timing e sincronizzazione. In questa applicazione, l'utilizzo di un sistema operativo general-purpose, invece di un RTOS, potrebbe causare accumulo di ritardi sull'intera linea di assemblaggio, o portare alla consegna all'utente finale di prodotti con parti difettose.

Fig. 4 – Fonte: Pixabay

Sviluppo del sistema: attenzione ad alcuni aspetti chiave

Quando si sceglie di usare un RTOS, un primo punto di difficoltà è relativo a quali priorità si devono assegnare ai diversi task, e quale di essi debba avere quella più alta. In questi casi, una buona pratica è evitare modalità di assegnazione delle priorità basate su proprie valutazioni personali di quali siano i task prioritari: meglio invece partire affidandosi a tecniche e algoritmi RMS (rate-monotonic scheduling), in grado di fornire già un buon punto di partenza, su cui si può successivamente lavorare per eseguire ulteriori e più precisi aggiustamenti delle priorità.
Altro aspetto cruciale è la fase di debugging del sistema embedded, che tipicamente occupa molto tempo e, nel caso di un RTOS, può complicarsi ulteriormente: ciò è dovuto all'insorgere di vari tipi di problemi, come, ad esempio, l'inversione di priorità, o gli stati di "deadlock", quelli in cui il sistema va in fase di di stallo, per la presenza di processi concorrenti nell'uso delle risorse. Per ovviare a problemi come questi e velocizzare il lavoro, è utile adottare tecniche e strumenti di tracciamento, in grado di registrare quali eventi si verificano nel sistema, quando i task vengono avviati e quando terminano l'esecuzione, e quant'altro è utile a comprendere il comportamento del RTOS. Ancora, è importante attuare una buona gestione della memoria, che in un RTOS embedded viene amministrata a diversi livelli, e tipicamente non è disponibile nelle quantità riscontrabili nelle normali macchine desktop commerciali, perché aggiungerla può significare il non rispetto di determinati requisiti in termini di peso, o costo del sistema. Dunque, soprattutto se il dispositivo embedded in questione dispone di risorse hardware limitate, occorre ridurre al massimo le dimensioni del codice del RTOS. Ad esempio, specie negli RTOS dotati di un ricco insieme di moduli e funzionalità, vanno disabilitate tutte quelle che non sono strettamente necessarie per l'applicazione, e che occupano molto spazio nella RAM. Altro fattore determinante è gestire in maniera corretta gli oggetti del RTOS, e la modalità con cui viene allocata la memoria del sistema: quest'ultima può essere assegnata in modalità statica, oppure dinamica (basata su heap). Le implementazioni "heap-based" possono tuttavia determinare un impatto sulle prestazioni real-time e sul comportamento deterministico del sistema embedded.

ITALIA 4.0

TECNOLOGIE PER LO SMART MANUFACTURING

www.italia40-plus.it

RIVISTA

In uscita a dicembre, sia in forma cartacea sia digitale, ha l'ambizione di essere un osservatorio privilegiato per fare il punto sull'anno che si sta per concludere ed analizzare i trend che caratterizzeranno il prossimo futuro.

Codifica per applicazioni sicure e protette

Sicurezza e protezione sono concetti differenti ma esistono modi in comune per ottenere entrambe nelle applicazioni ad alta integrità

Richard Bellairs
Product Marketing Manager
PRQA

Il mondo sta diventando via via sempre più connesso, e i sistemi sono quindi vulnerabili agli attacchi perpetrati attraverso le connessioni stesse. Ci sono già stati alcuni esempi, di elevato profilo, che hanno scosso il settore, al di là di eventuali compiacimenti che possano esserci stati.
La sicurezza (safety) nei sistemi ad elevata integrità è stata a lungo una priorità mentre la protezione (security) non ha ricevuto la medesima attenzione, anche se sicurezza e protezione devono soddisfare diversi set di regole e protocolli. Tuttavia, anche se sono intrinsecamente differenti, condividono alcuni temi comuni e, per questo motivo, quando si considerano gli aspetti di codifica, è possibile adottare un approccio olistico.
La necessità di affrontare queste questioni è presente in ogni applicazione, soprattutto in sistemi security critical, tuttavia, è difficile fornire una definizione formale di ciò che è sicuro e ciò che è protetto quando si parla di sviluppo software.
Esistono standard di sicurezza funzionale come IEC61508 o ISO26262 ma, confrontando i requisiti degli standard di codifica riconosciuti nel settore per i sistemi ad elevata integrazione con quelli per software di tipo security critical, il terreno comune tende progressivamente ad espandersi.
La discussione sulle caratteristiche relative a sicurezza e protezione in un linguaggio come C o C++ è limitata dalla natura del linguaggio stesso, quindi ciò che tende ad emergere sono stili e metodologie volti a preservare sicurezza e protezione nell'applicazione di uno di più standard di codifica.

Internet of (un)secure Things

La crescita del numero di dispositivi interconnessi in grado di fornire servizi avanzati, generalmente chiamati Internet of Things (IoT), è destinata ad aumentare in modo esponenziale nei prossimi anni. Mentre le promesse di efficienza e riduzione dei costi portati da questa evoluzione sono davvero attraenti, esse portano con loro problemi di notevole entità relativi alla sicurezza.
Il noto attacco dimostrativo che ha permesso a due ricercatori di assumere il controllo remoto di un moderno SUV, notizia ripresa in tutto il mondo, è stata un allarme sia per i produttori sia per i clienti: se un sistema tecnologicamente avanzato, come una moderna auto di fascia alta, può essere soggetta a questo tipo di attacco, che cosa può accadere alle apparecchiature interconnesse più comuni, di basso costo, che rappresenteranno la maggior parte dei molti miliardi sistemi che comporranno il crescente IoT?
Sebbene la minaccia sia ben chiara, l'integrazione della protezione come elemento basilare per guidare lo sviluppo e i processi aziendali in modo simile alla sicurezza funzionale è ancora di là da venire. Ciò è lungi dall'essere rassicurante data la quantità e il livello dei rischi offerti dalle vulnerabilità della sicurezza.

Il livello di processo (Process level)

Instillare una cultura dove i processi che preservano sicurezza e protezione coesistano in modo efficiente, richiede tempo e impegno. L'approccio da adottare è di natura olistica e non può essere limitato a singoli comparti o fasi di sviluppo. Ad esempio, l'attacco al SUV ha sfruttato le debolezze e le vulnerabilità a vari livelli, architettura, autorizzazioni, algoritmi di generazione delle password e così via. Di conseguenza, un processo di sviluppo

di un prodotto dovrebbe integrare azioni di rafforzamento della protezione a tutti i livelli e consentire loro di coesistere in modo efficiente con i già esigenti requisiti di sicurezza funzionale.
Ma cosa succede quando l'attenzione è posta solamente sullo sviluppo del software? Più in particolare, quali sono le scelte possibili per uno sviluppatore con il compito di programmare un'applicazione safety critical e con la necessità per essere certo che quell'applicazione sia anche protetta, oltre che sicura? Supponendo che siano state applicate tutte le possibili misure nei requisiti e fasi di progettazione, è il momento di scegliere la modalità per tradurli in un software efficiente, sicuro e di elevata integrità.

Fig. A – Numero stimato di dispositivi IoT installati suddivisi per settore applicativo (fonte: Business Insider Intelligence)

Approccio "safety critical"

La sicurezza funzionale prevede due principali famiglie di standard cui fare riferimento e che hanno a che fare con l'organizzazione del ciclo di vita del software: IEC61508 oltre agli standard derivati, e DO178B/C con documenti correlati, come il DO330. IEC61508 riguarda la sicurezza funzionale di sistemi safety-related di tipo elettrico, elettronico e programmable electronic (EEPE).
Esso copre rischi causati da avarie delle funzioni di sicurezza. Dal momento che può essere applicato a qualsiasi sistema safety-related che contenga un dispositivo EEPE, la sua portata è piuttosto ampia. Quasi tutti gli standard di sicurezza dei principali settori non collegati con l'Avionica sono derivati da IEC61508. DO178C, con i suoi documenti collegati, DO330, DO331, DO332 e DO333 formano gli standard per applicazioni avioniche. DO178C è obbligatoria per qualsiasi progetto di avionica commerciale che voglia ottenere la certificazione FAA.
DO178C è più focalizzato sul software rispetto IEC61508; il livello di sicurezza del software (o IDAL - item development assurance level) è determinato dall'analisi del rischio e dalla valutazione della sicurezza e mappato su cinque livelli, da A (catastrofico) a E (nessun effetto). Per applicazioni safety-critical, la definizione delle criticità del codice è stata ampiamente analizzata e ci sono metodi standardizzati per qualificarla e definire modi adeguati per gestire il processo di sviluppo. Safety integrity levels (SIL) in IEC61508, Automotive SIL (ASIL) in ISO26262, software SIL (SSIL) in EN50128 o IDAL in DO178C, sono tutti esempi dello stesso concetto per quantificare la riduzione del rischio necessaria per una funzione, in base all'analisi di rischio e decidere le azioni *qualified* da intraprendere per assicurare che tale livello sia raggiunto.
Quasi tutti gli standard di sicurezza funzionale riconosciuti prescrivono l'adozione di standard di progettazione e codifica in base al SIL target. Sebbene non ci sia alcuna indicazione autorevole su quale standard di codifica sia adatto per la sicurezza funzionale, uno dei principali riferimenti in questo ambito è MISRA C.
ISO26262-6 riconosce per il linguaggio C che MISRA C copre molti dei metodi richiesti per il software unit design e l'implementazione, e la sua diffusione raggiunge tutte le principali applicazioni safety critical, quali macchinari, medicali, energia nucleare e ferroviario.
Con DO178B/C, la situazione non è molto diversa. Questi standard richiedono una accurata definizione e documentazione del processo di sviluppo del software. Il set base della documentazione e lifecycle artefacts richiesti comprende una ricca e dettagliata pianificazione, e applicazione standard di codifica è parte di questo elenco.

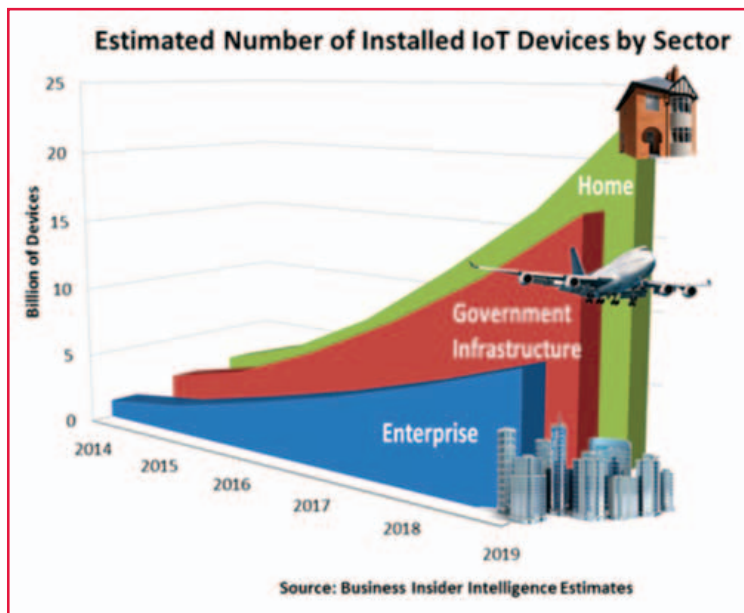
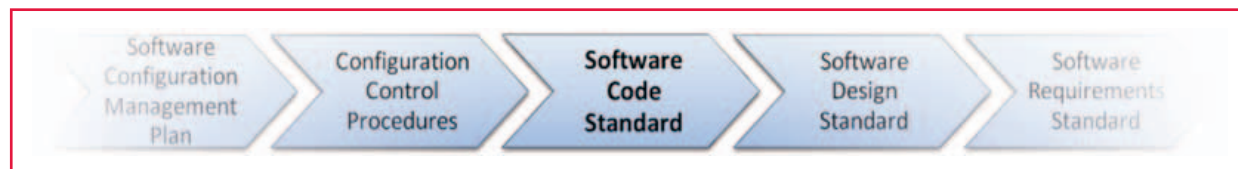



Fig. B – Standard come DO178B/C richiedono un'accurata definizione e documentazione del processo di sviluppo del software

Standard di codifica come MISRA definiscono un sottoinsieme del linguaggio di destinazione. Questo evita o limita l'utilizzo di funzioni e costrutti che potrebbero portare ad un comportamento non definito o non specificato. In genere sono scoraggiate pratiche come tollerare la presenza di dead code o di codice irraggiungibile, che può causare problemi quando si considera la tracciabilità e verifica.
Gli standard di codifica per le applicazioni ad alta integrità tendono a far rispettare le caratteristiche che offrono un comportamento prevedibile. MISRA C:2012, ad esempio, sconsiglia l'utilizzo di memoria dinamica per il fatto che un uso improprio dei servizi di libreria standard per gestire la memoria allocata in modo dinamico può portare a comportamenti non definiti. Quando si sceglie di farlo, si dovrebbe prestare particolare attenzione per evitare esiti imprevedibili.

Sicurezza dell'applicazione (Application security)

ISO/IEC27001: 2003 specifica i requisiti per stabilire, implementare, mantenere e migliorare con continuità un sistema di gestione della sicurezza delle informazioni. È basato sul modello PDCA (*plan, do, check, act*), condiviso con tutti i principali standard di gestione. Valutazione del rischio e analisi di impatto sul business vengono utilizzati per identificare e gestire i possibili rischi per la riservatezza, l'integrità e la disponibilità delle informazioni.
Uno sguardo più dettagliato sulla sicurezza dell'applicazione viene offerto da ISO/IEC27034:2011, che fornisce una guida nella definizione e implementazione dei controlli di sicurezza delle informazioni attraverso processi integrati nel *lifecycle* dello sviluppo del sistema.
Come tale, esso non è uno sviluppo di applicazioni software standard, ma si basa su standard esistenti. Spostandosi verso gli standard di codifica security-oriented, lo scenario è molto vario; si incontrano norme di codifica sicure per C e C+, così come per Java, Perl, PL/SQL e altri. C'è un'ampia varietà di tecniche disponibili per valutare la sicurezza del codice. Diversi problemi possono essere rintracciati usando analisi statica, dinamica e valutazione di runtime, data flow e control flow tracking, taint analysis, analisi dell'eseguibile e analisi euristica. Queste tecniche possono essere efficaci e facili da attuare a seconda del supporto esistente per la lingua selezionata, strutture integrate, librerie, e così via.
Il punto di riferimento principale per la sicurezza degli standard di codifica è CERT, che per molti anni ha pubblicato norme di codifica volte alla tutela della sicurezza.
Le norme di codifica CERT direttamente derivate dalle vulnerabilità del mondo reale, e classificate dal common weaknesses enumeration (CWE). Il CWE è un dizionario delle vulnerabilità sviluppato da una intera comunità. L'elenco scaricabile dei punti di vulnerabilità può essere esplorato secondo contesti di relazione specifici.
Il CWE è legato ad un più ampio insieme di vulnerabilità della sicurezza dei dati, noti pubblicamente, conosciute come CVE (common vulnerabilities and exposures), che è ora lo standard per la normale identificazione delle vulnerabilità. Gli identificatori CVE, noti anche come CVE ID, forniscono punti di riferimento per lo scambio dati dei servizi e prodotti per la sicurezza. Essi sono utili per analisi di coverage e dell'efficacia di strumenti e servizi in relazione a specifiche classi di vulnerabilità.
Il database nazionale delle vulnerabilità del NIST, il depositario per il governo federale degli Stati Uniti dei dati di gestione della vulnerabilità basati su standard, contiene più di 73.000 CVE.

MISRA vs CERT

MISRA C:2012 e CERT C possono essere considerati campioni della sicurezza e protezione per il linguaggio C. Un sintetico raffronto è riportato in tabella 1.

Tab. 1 – Confronto tra CERT e MISRA		
	MISRA C:2012	CERT C
Analisi	**Restrizioni (gruppo di lavoro)**	**Aperto e pubblico (web)**
Struttura	143 Rules / 16 Directives Le Roles sono linee guida per le quali è stata fornita una descrizione completa dei requisiti. Le Directives sono linee guida per le quali non è possibile fornire la completa descrizione necesaria per eseguire una verifica della conformità.	98 Rules / 178 Recommendations Le Rules sono definite in base a tre criteri: 1. La violazione delle linee guida è probabile diventi un difetto della sicurezza 2. Non si basano su annotazioni al codice sorgente o su ipotesi di intenti del programmatore 3. La conformità alle linee guida può essere determinata mediante analisi automatica, metodi formali, o ispezione manuale Le *Recommendations* sono definite in base a due criteri: 1. La loro applicazione è verosimile che migiori la sicurezza, l'affidabilità o la protezione dei sistemi software. 2. Uno o più dei requisiti da indicare come rule non possono essere soddisfatte.
Applicazione	La formulazione delle rules è orientata verso una applicazione automatizzata Es.: Rule 8.14 "i Qualifier riservati non dovranno essere utilizzati"	La formulazione delle Rules è appena più generica. Es.: EXP43-C: "Nell'utilizzare i puntatori *restrict-qualified* vanno evitati i comportamenti non definiti"
Organizzazione	Per settori di linguaggio e ambiente: "The Implementation", "Compilation and build", "Requirements traceability", "Code design", "A standard C environment", "Unused code", "Comments", "Character sets and lexical conventions", "Identifiers", "Types", "Literals and constants", "Declarations and definitions", "Initialization", "The essential type model", "Pointer type conversions", "Expressions", "Side effects", "Control statement expressions", "Control flow", "Switch statement", "Functions", "Pointers and arrays", "Overlapping storage", "Preprocessing directives", "Standard libraries" and "Resources".	Per elementi di linguaggio di basso livello: "Preprocessor (PRE)", "Declarations and initialization (DCL)", "Expressions (EXP)", "Integers (INT)", "Floating Point (FLP)", "Arrays (ARR)", "Characters and strings (STR)", "Memory management (MEM)", "Input/Output (FIO)", "Environment (ENV)", "Signals (SIG)", "Error handling (ERR)", "Application Programming Interfaces (API)", "Concurrency (CON)", "Miscellaneous (MSC)", "POSIX (POS)", "Microsoft Windows (WIN)"
Severity classification	Liberamente collegato alle proprietà di "Category" della Rule: • Mandatory (nessuna deroga ammessa) • Required (deroghe consentite) • Advisory (processi di deroga formale non richiesti)	Approccio basato sulla valutazione dei rischi. Ogni linea guida ha una *priority* come prodotto di *severity*, *likelihood* e *remediation cost* (ciascuno di essi con un valore in una scala da 1 a 3). La gamma di priorità definisce il legame con uno dei tre livelli possibili: L1 -> Priorities 12, 18, 27 (elevata severità) L2 -> Priorities 6, 8, 9 L3 -> Priorities 1, 2, 3, 4 (bassa severità)
Procedura di Deroga	Formalizzato: richiede l'indicazione della linea guida da cui si è derogato, le circostanze in cui è consentita la deroga, la motivazione della deroga, una valutazione del rischio derivante (dimostrazione di come la sicurezza è ugualmente assicurata, ulteriori prove richieste ecc.) ed è necessaria una approvazione formale. Limitata: è possibile derogare solo da Rules di tipo Advisory e Required.	Non c'è alcuna descrizione di un formale processo di gestione per le deroghe, anche se sono menzionati come un modo per sopprimere i veri e veri-positivi dimostratamente innocui o che sono in accadimento sulle scelte architetturali non previste dallo standard.

Ci sono differenze notevoli tra gli standard CERT e MISRA, ma è possibile definire una strategia che comporti l'applicazione efficace di entrambi sul medesimo codebase. Strumenti come quelli offerti da PRQA sono il modo più efficace per attuare tale strategia. Tali strumenti eseguono approfondite analisi del codice software per prevenire, rilevare ed eliminare i difetti e applicare automaticamente regole di codifica per garantire la conformità agli standard. Portano con sé il beneficio aggiunto della migliorata manutenibilità del software e quindi della riduzione dei costi complessivi di sviluppo.

Considerazioni conclusive

Progettare un'applicazione safety-critical ottimizzando al contempo anche la sicurezza può essere impegnativo.
Sicurezza e protezione richiedono un insieme di strategie, processi, strumenti e competenze che possono non sovrapporsi del tutto o, addirittura, risultare in conflitto. Strumenti di analisi automatizzata del codice sono un modo efficace per evitare difetti nella codifica che possono portare a problemi e a vulnerabilità sia della sicurezza sia della protezione, come parte di un approccio olistico.

Come proteggere le smart factory del futuro

L'adozione della tecnologia che prevede l'uso di Separation Kernel permette di controllare l'interfacciamento tra due domini tradizionalmente separati, il mondo OT e quello IT, fornendo un'arma di difesa efficace contro gli attacchi di natura informatica

Lee Cresswell
Sales Director - EMEA
Lynx Software Technologies

La storia è costellata di esempi di attacchi informatici contro infrastrutture industriali. Anche se si tratta di un numero abbastanza limitato e con cadenze temporali non ravvicinate, ritenere che queste minacce rimangano incidenti isolati può essere un'ipotesi pericolosa.
Alcuni attacchi informatici appaiono del tutto immotivati, condotti solo per il gusto di fare un atto di sabotaggio o forse per affermare la futura credibilità di un ricattatore che ha condotto l' attacco tramite ransomware.
Un attacco di questo tipo è stato registrato nel novembre del 2011: in questo caso gli hacker hanno rubato le password che hanno poi utilizzato per accedere a un sistena SCADA (Supervisory Control And Data Acquisition) appartenente a Water Utility[1]. In questo caso si pensa abbiano distrutto una pompa utilizzata per convogliare l'acqua a migliaia di abitazioni in una cittadina statunitense nello Stato dell'Illinis aprendola e richiudendola rapidamente. Alla fine del 2014 un'acciaieria tedesca è stata l'obiettivo di un attacco informatico analogo: anche in questo caso gli hacker hanno preso di mira un sistema SCADA che ha prodotto ingenti danni materiali al sito produttivo[2]. Gli intrusori hanno dapprima violato una rete interna del sito che hanno utilizzato per accedere al software che gestisce la produzione dell'acciaieria. Da lì gli hacker hanno preso il controllo della maggior parte dei sistemi di controllo dell'impianto e distrutto metodicamente i componenti che governano l'interazione tra uomo e macchina. In questo modo hanno impedito che un altoforno potesse iniziare nei tempi previsti le procedure di sicurezza provocando in tal modo gravi danni all'infrastruttura.
In altri casi gli attacchi sembravano avere un movente di natura politica. Il 23 dicembre 2015, ad esempio, intrusori sono entrati nei sistemi SCADA ucraini per togliere l'energia a 17 sottostazioni e impedire l'accesso alle linee telefoniche della società per ritardare il ripristino dell'energia[3]. Parecchi mesi prima che si verificasse l'attacco, gli hacker avevano iniziato a inviare e-mail a scopo di pishing agli uffici delle società che gestivano la distribuzione dell'energia in Ucraina. Una volta aperti, questi messaggi di posta elettronica installavano il malware. I firewall erano stati progettati per separare i computer affetti da virus dai sistemi di controllo dell'energia, ma il malware noto come BlackEnergy 3 ha consentito agli hacker di acquisire password e log-in con le quali sono stati in grado di condurre l'attacco contro il sistema SDA stesso.
Alcuni anni prima, nel 2010, un attacco Stuxnet, ampiamente documentato, ha rappresentato un esempio di malware sofisticato che aveva come obbiettivo un bersaglio specifico e ben protetto, l'impianto di arricchimento dell'uranio di Natanz in Iran[4]. Non solo l'attacco ha conseguito l'obiettivo, ma ha anche provocato danni significativi all'impianto, tanto da essere definito dai media come la "prima arma digitale".
Quelli appena descritti sono quattro esempi di attacchi informatici contro infrastrutture "safety-critical" in vari settori industriali. Nonostante

Fig. 1 – Modello dell'architettura di riferimento per Industry 4.0 (RAMI 4.0)(6)

si tratti di attacchi di natura diversa, l'esistenza di una strada d'accesso tra Internet e un dominio "safety critical" è il denominatore comune di questi esempi.

Interoperabilità sicura e protetta

Le organizzazioni che si occupano degli aspetti legati all'ingegnerizzazione forniscono numerose indicazioni quando si tratta di progettare, sviluppare e installare una rete Internet industriale che risulti interoperabile, sicura (safety) e protetta (security). In particolare IIC (Industrial Internet Consortium) e il Working Group for Industrie 4.0 hanno prodotto linee guida e raccomandazioni sotto forma rispettivamente dell'architettura IIRA (Industrial Internet Reference Architecture) e del modello RAMI 4.0 (Reference Architectural Model for Industrie 4.0). È abbastanza ovvio che vista la somiglianza tra gli obiettivi che si propongono i due documenti, esistono similitudini e sovrapposizioni, come d'altro canto si evince dalle discussioni in corso tra le due organizzazioni.
Entrambe in ogni caso riconoscono che un elevato livello di protezione è essenziale per le applicazioni IoT in ambito industriale (IoT). IIC ha introdotto l'Industrial Internet Security Framework (IISF)[5] con l'obiettivo di fornire alcune line guida a questo riguardo e poiché questi due organismi cooperano per raggiungere l'armonizzazione in un certo numero di aree, la protezione è stata identificata come fattore chiave.
Le problematiche relative alla sicurezza possono essere comprese facendo riferimento a un impianto generico in cui convergono molte richieste sulle infrastrutture dei sistemi. I sensori permettono ai responsabili delle operazioni di raccogliere dati come ad esempio localizzazione, posizione, velocità, temperatura, stato di blocco e vibrazioni di tutti i loro asset praticamente in tempo reale. Con un livello di sicurezza più elevato, le impostazioni dell'impianto o persino il firmware possono essere aggiornate in modo remoto in risposta ai dati forniti da questi sensori o al mutamento delle richieste in produzione. I dati relativi alla produzione e alla profittabilità rappresentano un problema differente, di natura prettamente commerciale: le informazioni sensibili devono essere separate dai dati di natura ingegneristica provenienti dai sensori.
Nel modello RAMI 4.0 tali considerazioni vengono astratte in una matrice a tre dimensioni (Fig. 1) formata da strati (Layers), ciclo di vita e flusso del valore (Life Cycle & Value Stream) e livelli gerarchici (Hierarchy).
Si tratta di una rappresentazione straordinariamente simile ai domini funzionali (Functional Domain) e ai punti di vista (Viewpoint) del modello IIRA proposto dal consorzio IIC (Fig. 2).
Per comprendere il modo migliore per fornire una base sicura per entrambi gli schemi, è utile riflettere sul fatto che le astrazioni appena riportate rappresentano l'unione di due mondi tradizionalmente distinti: quello della tecnologia operativa (OT - Operational Technology) e quello della tecnologia dell'informazione (IT - Information Technology). Per quanto riguarda la tecnologia OT, la protezione è integrata in virtù del fatto che essa, oltre a essere isolata, solitamente è di tipo proprietario mentre la tecnologia IT è focalizzata sulla protezione delle risorse (asset) aziendali. L'abbinamento tra le due tecnologie minaccia la sicurezza di entrambi i sistemi in quanto mette a disposizione un potenziale mezzo di accesso a potenziali minacce che non sono in grado di affrontare.
In ogni caso è chiaro che a prescindere da qualsiasi differenza e somiglianza tra le due architetture, l'isolamento di un dominio dall'altro è una caratteristica fondamentale di qualsiasi imple-

mentazione conforme. In particolare, la separazione dei dati è essenziale per garantire l'accessibilità solo a chi ne è autorizzato. A questo punto val la pena sottolineare che i dati sono l'elemento che consentono un funzionamento corretto e sicuro delle applicazioni IIoT. Di conseguenza il valore intrinseco del sistema è generato nei punti terminali (endpoint), sia che si tratti di un database contabile o della lettura del valore di temperature fornito da un sensore.
Per non compromettere fonti di dati così eterogenee, un'applicazione IIOT deve non solo fornire alla tecnologia OT i livelli di protezione, resistenza e affidabilità stabiliti ma anche innalzare i livelli di riservatezza e protezione in modo da proteggere in modo adeguato la tecnologia IT. Quest'ultima, dal canto suo, dovrà assicurare livelli di resistenza e sicurezza più elevati per garantire le eccellenti caratteristiche di riservatezza, protezione e affidabilità intrinseche della tecnologia stessa. Tutto ciò potrebbe essere realizzabile se tutti questi sistemi interconnessi fossero realizzati a partire da zero prevedendo questo modello di connettività. Ovviamente non si tratta di un'ipotesi percorribile. Un approccio migliore è proteggere i punti terminali per mezzo di un gateway basato sul concetto di kernel a separazione (SK - Separation Kernel).

Separation Kernel

Sebbene un approccio di questi tipo è basato su principi che forse rappresentano una novità per il settore industriale, esso è ampiamente utilizzato in altri comparti. I Separation Kernel hanno protetto informazioni riservate nei sistemi di comunicazione governativi per un decennio e val la pena quindi riflettere sui principi, di origine accademica, che hanno reso possibile un tale successo. Il concetto di Separation Kernel è stato introdotto nel 1981 da John Rushby[8], il quale suggeriva che esso dovrebbe essere formato da "una combinazione di hardware e software che permetta l'implementazione di più funzioni sfruttando un insieme comune di risorse fisiche senza dar luogo a interferenze mutue non desiderate". Queste argomentazioni sono state convincenti a tal punto che il principio del Separation Kernel costituisce la base dell'iniziativa MILS (Multiple Independent Levels of Security). In modo del tutto analogo, circa trent'anni fa, Saltzer e Schroeder[9] affermavano che "ogni programma e ogni utente del sistema dovrebbero agire utilizzando l'insieme minimo di privilegi necessari per portare a termine il proprio compito ".
Questo approccio che utilizza il concetto di "Least Privilege" (minimo privilegio) diventa inderogabile laddove sono presenti applicazioni contraddistinte da differenti livelli di criticità che girano a stretto contatto le une con le altre. I concetti di Separation Kernel e Least Privilege sono quindi focalizzati sui vantaggi della modularità, con il primo che fa riferimento alle risorse e il secondo che fa riferimento alla funzionalità del sistema - un aspetto tenuto in considerazione anche da Levin, Irvine e Nguyen nel loro paper "Least Privilege in Separation Kernels"[10] dove hanno proposto un mix tra i due concetti. Nella figura 3 è schematizzata l'applicazione del principio del minimo privilegio ai "Subjects" (entità attive eseguibili) e "Resources" (risorse) che sono sovrapposti ai blocchi del Separation Kernel, evidenziando la granularità del controllo del flusso a livello di risorse e di soggetto.

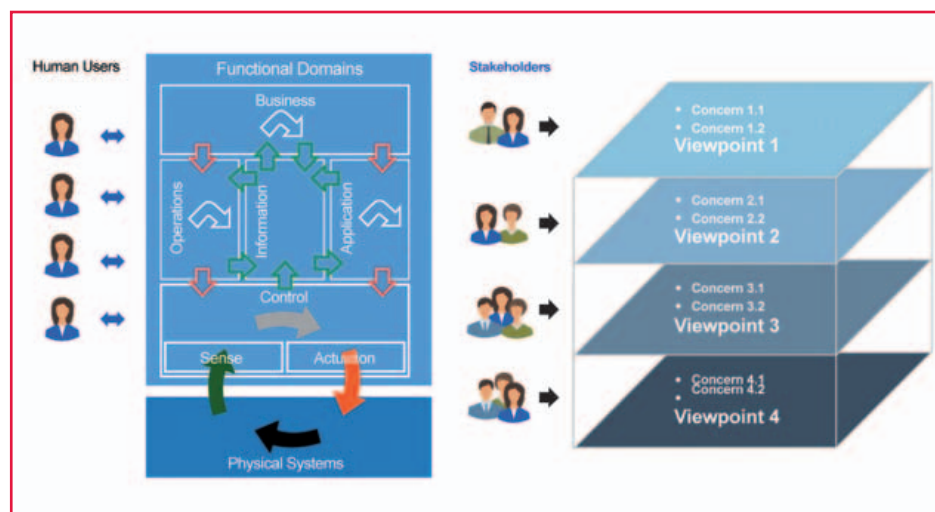



Fig. 2 – Rappresentazione dei "Functional Domains" e dei " Viewpoints"(7) previsti dal modello IIC

Virtualizzazione hardware

Sebbene i principi alla base del Separation Kernel e del concetto di minimo privilegio sono ampiamente sperimentati, i primi tentativi di implementazione erano basati sulla virtualizzazione software che, oltre a fornire prestazioni non soddisfacenti, non era in grado di supportare le applicazioni real time. La diffusione del concetto di virtualizzazione a livello aziendale ha spinto i maggiori produttori di silicio (tra cui Intel, AMD e ARM) ad aumentare il numero di core per CPU e implementare un supporto avanzato per la virtualizzazione in hardware. A questo punto, il concetto di Separation Kernel si è trasformata da un'idea teorica in una proposta pratica. Esistono numerosi hypervisor embedded che si propongono di raggiungere obiettivi simili basati su un'architettura modificata del sistema operativo. In ogni caso, per ottimizzare le credenziali di sicurezza di un Separation Kernel, è necessario distribuire i principi del minimo provilegio per minimizzare la base di elaborazione sicura (TCB - Trusted Computing Base) e quindi la superficie di attacco al fine di migliorare la protezione fornita dal gateway.

Fig. 3 – La sovrapposizione dei principi del minimo privilegio (Least Provilege) sui blocchi dell'SK garantisce una granularità molto fine in termini di controllo del flusso a livello di risorse e soggetto

Separation Kernel: un esempio pratico

Per fare un esempio pratico dei concetti appena esposti, si consideri un tornio che deve generare dati di produzione (Fig. 4). Tali dati, a loro volta, verranno condivisi, attraverso il cloud, con il responsabile di turno dell'impianto. In questo esempio il soggetto che si interfaccia al cloud potrebbe essere un sistema operativo di tipo general purpose, come Windows o Linux, potenzialmente vulnerabile ad attacchi di hacker. L'aspetto importante è rappresentato dal fatto che gli hacker non possono accedere al soggetto che si interfaccia con l'impianto - che può essere un RTOS o un'applicazione di tipo "bare-metal - anche se il soggetto che si interfaccia al cloud risulta compromesso.

Un Separation Kernel implementato in conformità ai principi del minimo privilegio avrà caratteristiche tali da risultare la scelta ottimale in questo tipo di applicazione in termini di:

• Velocità

Per garantire prestazioni assimilabili a quelle native, il Separation Kernel dovrà introdurre il minimo overhead possibile e sfruttare al massimo le caratteristiche di virtualizzazione dell'hardware.

• Dimensioni ridotte

Per garantire che i servizi del sistema operativo come gestione di processi, I/O e driver siano controllate dai soggetti, il Separation Kernel dovrà essere molto "leggero" e meno vulnerabile agli attacchi

• Praticità

Il Separation Kernel supporterà il riutilizzo del software legacy mettendo a disposizione dei soggetti una "scheda madre virtuale" in modo che i soggetti stessi possano essere installati ed eseguiti proprio come se si trattasse di un'installazione nativa

• Sicurezza

La configurazione di tipo statico garantirà che il Separation Kernel risulti immutabile una volta realizzato e installato e sarà caratterizzato da una superficie di attacco minima.

La difesa contro Stuxnet

L'attacco con il virus Stuxnet rappresenta un ottimo esempio della modalità di utilizzo della

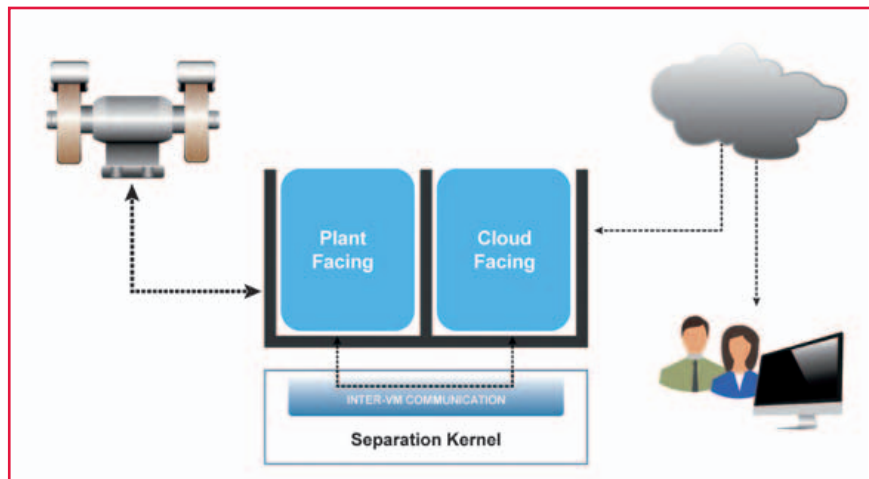



Fig. 4 – Esempio di un'applicazione pratica del concetto di Separation Kernel

tecnologia del Separation Kernel per la difesa di infrastrutture critiche in un'applicazione pratica. Obiettivo di Stuxnet era infettare e quindi manipolare i PLC (Programmable Logic Controller) di Siemens, ovvero questi sistemi di elaborazione embedded che eseguono il controllo e il monitoraggio della velocità delle centrifughe che arricchiscono l'uranio e girano a velocità elevatissime. Questi sistemi non erano collegati direttamente a Internet per cui è stato necessario mettere a punto sofisticato un processo di infezione mediante malware per trasportare il "carico utile" verso il bersaglio e portare a termine l'attacco. Gli intrusori hanno usato le classiche tecniche di infezione tramite malware come ad esempio chiavette USB infette e chiamate telefoniche per infiltrarsi e quindi analizzare i sistemi collegati alla rete sicura finché non sono arrivati ai PLC che controllavano le centrifughe. Un Separation Kernel distribuito all'interno dell'impianto avrebbe rappresentato un serio ostacolo al progredire dell'infezione finalizzata alla ricerca del proprio bersaglio. In uno scenario di questo tipo il computer interfacciato ai PLC Siemens che rappresentavano il punto terminale avrebbe avuto il massimo livello di protezione possibile, compresa la disabilitazione di qualsiasi porta (come ad esempio una porta USB) che avrebbe consentito l'accesso ai file dannosi di entrare nel proprio dominio.

Considerazioni conclusive

Benché gli attacchi informatici non siano un evento che si verifica quotidianamente, i danni potenziali che possono provocare sono potenzialmente illimitati. Come evidenziato in questo articolo, gli attacchi condotti contro infrastrutture di vario tipo - acciaierie, impianti per la distribuzione dell'acqua, siti per l'arricchimento dell'uranio e reti di distribuzione dell'energia elettrica - sono una chiara dimostrazione che tutti i settori industriali possono rappresentare potenziali bersagli di attacchi da parte di hacker. Il comune denominatore di questi attacchi è la presenza di un percorso vulnerabile che consente l'accesso ai sistemi che si interfacciano con l'esterno connessi a Internet e ai sistemi "safety critical" dell'impianto stesso. Come evidenziato da IIRA (Industrial Internet Reference Architecture) e RAMI 4.0 (Reference Architectural Model for Industrie 4.0), tali vulnerabilità sono il frutto della necessità di unire due mondi, quello IT e quello OT, tradizionalmente separati. L'adozione della tecnologia che prevede l'uso di Separation Kernel permette di controllare questo interfacciamento, fornendo un'arma di difesa efficace contro gli attacchi di natura informatica.

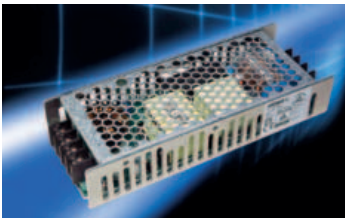
Note

[1] http://www.bbc.co.uk/news/technology-15817335
[2] http://www.bbc.co.uk/news/technology-30575104
[3] http://www.bbc.co.uk/news/technology-35686493
[4] http://www.bbc.co.uk/timelines/zc6fbk7
[5] http://www.iiconsortium.org/IISF.htm
[6] Umsetzungsstrategie Industrie 4.0 – Ergebnisbericht, Berlin, April 2015
[7] Industrial Internet consortium – Industrial Internet Reference Architecture version 1.7. 4th June, 2015.
[8] Rushby, J. Design and Verification of Secure Systems. Operating Systems Review. 15(5). 1981.
[9] Saltzer, J.H. and Schroeder, M.D. The Protection of Information in Operating Systems. Proceedings of the IEEE 63(9):1278-1308. 1975.
[10] Levin, T.E., Irvine C.E. and Nguyen T.D. Least Privilege in Separation Kernels. Department of Computer Science, U.S. Naval Postgraduate School. 2004.

I connettori per risparmiare tempo

I connettori per FPC (Flexible Printed Circuit)/FFC (Flexible Flat Cable) di **Omron Electronics** dotati di sistema BackLock, il meccanismo bloccacavo che utilizza un cursore rotante, offrono la possibilità di ridurre i tempi di assemblaggio sulle linee produttive, con i relativi vantaggi in termini economici.
Molti produttori, infatti, offrono i connettori FPC con il fermo bloccacavo in posizione chiusa ma il meccanismo previsto da Omron permette di fornire il connettore con il fermo in posizione aperta rendendo più veloce l'assemblaggio. Il sistema di ritenzione, inoltre, è stato progettato per fornire una connessione affidabile e la protezione del cavo. La gamma comprende connettori da 6 a 60 pin offerti su bobine da 100 o 1.500 pezzi. Il passo varia da 0,25 mm a 0,5 mm. Le possibili applicazioni comprendono dispositivi wearable, smartphone, proiettori, unità a ultrasuoni, prodotti di sicurezza e moduli embedded.

Le nuove Target Board a basso costo

Renesas Electronics Corporation ha annunciato la disponibilità di tre nuove Target Board rispettivamente per i microcontroller RX65N, RX130 e RX231, ciascuna progettata per aiutare a raggiungere velocemente la massima efficienza nello sviluppo di elettrodomestici con interfaccia touch e applicazioni per automazione sia industriale sia civile. Ogni kit di sviluppo include uno strumento di debug on-chip che consente la progettazione dell'applicazione senza richiedere investimenti in ulteriori strumenti. Le connessioni per i pin di tipo "through-hole" consentono l'accesso a tutti i segnali del microcontroller, facilitando l'interconnessione con le breadboard standard per la prototipazione rapida. Le RX Target Board offrono, fra l'altro, una demo di codice sorgente e varie note applicative. Prossimamente saranno disponibili ulteriori varianti di Target Board che forniranno la copertura completa dell'intera famiglia RX, dalla serie RX100 a basso consumo alle serie RX700 a più alte prestazioni.

Alimentatori con potenza di picco fino a 206 W

TDK ha presentato la serie di alimentatori Lambda CUS200LD. Sono unità AC/DC con potenza di 120 W se usati con raffreddamento convenzionale e 150 W se invece si utilizza una base di alluminio per raffreddamento per conduzione. Il livello massimo è di 206 W per 10 secondi. La tensione di ingresso in alternata va da 85 CV a 265 V, mentre per l'uscita i valori disponibili sono di 5 V, 7,5 V, 12 V, 15 V, 24 V e 48 V. Il package è di tipo low profile e misura 160 x 60 x 31mm. Per le temperature operative, tutti i modelli della serie CUS200LD hanno una temperatura di start up di -40 °C e possono funzionare in una gamma di temperature comprese fra -20 e +70 °C, con un derating da +45 °C (raffreddamento a conduzione) fino al 40% a 70 °C. Le possibilità di impiego spaziano dalle applicazioni di LED signage a quelle industriali, ma anche broadcast, T&M e dispositivi per le comunicazioni.

Le nuove schede SD e microSD

Transcend Information ha annunciato la disponibilità delle nuove schede SD e microSD serie 500S e serie 300S. Le schede della serie SD 300S hanno una capacità da 16 GB a 512 GB mentre le schede microSD della serie 300S vanno invece da 16 GB a 128 GB. I modelli SD 500S offrono capacità da 8 GB a 256 GB e le schede microSD 500S da 8 GB a 128 GB. La velocità di trasferimento dichiarata da produttore per la serie 300S supera i 95 MB/s in velocità di lettura e 45 MB/s in scrittura (60 MB/s per la serie 500S). Le schede microSD da 128 GB, serie 300S soddisfano i più recenti standard Application Performance Class 1 (A1) della SD Association per la reattività. La serie Gold 500S, costruita con flash MLC, è particolarmente interessante per le action camera e i droni grazie anche all'elevata resistenza. Le schede SD e micro SD della serie 300S argento sono invece state progettate per il mercato degli smartphone.

Everyware IoT

Open. Integrated. Managed.

Business Application and IoT Services Integration

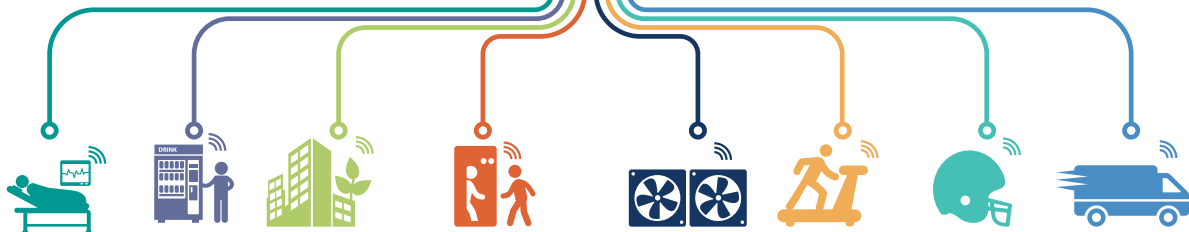
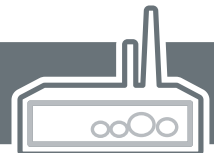
IoT Integration Platform

EC

IoT Communication Protocols

IoT Edge Framework

ESF

IoT Edge Gateways

Embedded IoT Made Easy

From field devices to the cloud, Everyware IoT simplifies and accelerates the development and deployment of your Internet of Things projects by providing best-in-class hardware and software building blocks

www.eurotech.com

Download our
IoT INFOGRAPHIC
eurotech.com/iot_infographic